Crosscutting Issues in International Transformation

Interactions and Innovations among People, Organizations, Processes, and Technology

Edited by Derrick Neal, Henrik Friman,
Ralph Doughty, and Linton Wells II

		Form Approved OMB No. 0704-0188
Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **DEC 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**
4. TITLE AND SUBTITLE **Crosscutting Issues in International Transformation. Interactions and Innovations among People, Organizations, Processes,and Technology**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,Washington,DC,20319-5066**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**2887**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

The views expressed in these essays are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government. All information and sources were drawn from unclassified materials.

Portions of this book may be quoted or reprinted without permission, provided that a standard source credit line is included.

Contents

Foreword

This book is a compilation of papers presented at the International Transformation Conference in Stockholm, Sweden on June 2–3, 2009. The conference was hosted by the Swedish Defence Research Agency at their Division of Information Systems in Kista. The papers are organized according to the categories of culture, interagency, transformation initiatives, leadership, and adaptive organizations. This sequence was chosen to group papers with common themes so that readers could follow the logic and findings of each paper more easily.

The book represents the views of the authors, most of whom are members of the International Transformation Chairs Network that was founded in the United States in 2004 by retired Vice Admiral Arthur K. Cebrowski, who then served as the Director of the U.S. Department of Defense Office of Force Transformation. Since that time, the organization has added members from the United Kingdom, Sweden, Australia, Singapore, and NATO.

The mission of the International Chairs Network is to provide a forum to challenge thinking, leverage shared knowledge, and inform the debate about the international security implications of global transformation. The vision of the group is that the efforts of these types of activities will ultimately result in a group of national security leaders who are prepared for a future filled with complexity, chaos, and surprise. Publication of this book is one step in the process of reaching this goal.

We hope that this book is valuable to you as you seek to transform your part of the world.

Ralph O. Doughty, Ph.D.
MG USA (Ret)

Martin Rantzer

Chair of Interagency and
Multinational Studies,
U.S. Army Command and
General Staff College

Director, Information Systems
Division,
Swedish Defence Research
Agency, FOI

v

VICE ADMIRAL ARTHUR K. CEBROWSKI

portrait by Margaret Holland Sargent
image courtesy of www.sargentportraits.com.

Vice Admiral Arthur Cebrowski—A True Transformative Leader

T he International Transformation Chairs recognize the contributions of Vice Admiral Arthur Cebrowski to the transformation process and pay tribute to him for his role in creating the International Transformation Network.

Vice Admiral (ret.) Arthur K. Cebrowski (August 13, 1942–November 12, 2005) served from October 2001 to January 2005 as Director of the Office of Force Transformation in the U.S. Department of Defense. In this position, he reported directly to the Secretary and Deputy Secretary of Defense and was responsible for serving as an advocate, focal point, and catalyst for the transformation of the U.S. military.

The Secretary of Defense called for the creation of the Office of Force Transformation in support of President George W. Bush's broad mandate to transform the Nation's military capabilities. The transformation process challenges the status quo with new concepts for American defense to promote an overwhelming and continuing competitive advantage for America's military.

As Director of the Office of Force Transformation, Admiral Cebrowski worked to link transformation to strategic functions, evaluated the transformation efforts of the military departments, and promoted synergy by recommending steps to integrate ongoing transformation activities. Among his primary responsibilities, Admiral Cebrowski monitored service and joint experimentation programs and made policy recommendations to the Secretary and Deputy Secretary of Defense.

We are indebted to Admiral Cebrowski for his vision and his initiatives to institutionalize effective transformation in the U.S. military. His contributions live on through the International Transformation Chairs Network and others who have benefited from his thinking.

The International Transformation Chairs Network

Transformation Chairs meeting, U.S. Air Force Academy, fall 2008

The International Transformation Chairs Network has evolved from the Transformation Chair system set up by the U.S. Office of the Secretary of Defense (OSD) through the Office of Force Transformation under the tutelage of Vice Admiral Cebrowski. The mission of the network is to "provide a forum to challenge thinking, leverage shared knowledge and inform the debate about the national and international security implications of global transformation."

The organization's vision is to "assist national security leaders and decision-makers in preparing for a future filled with complexity, chaos, and surprise."

The complexities of the task make definitions of transformation a challenge and often open to debate. The unpredictable nature of the future international security environment defies a tightly bounded definition so the International Transformation Chairs have adopted an inclusive description: "Transformation is a process that shapes the changing nature of competition and cooperation through new combinations of concepts, capabilities, people, and organizations."

The Transformation Chairs Network was created by the Secretary of Defense in 2004 to support the transformation of American defense concepts that was being implemented through the Office of Force Transformation (OFT). The underlying precept that drove the concept was the need to move transformational thinking down into the heart of the military organizations, principally through the education system, to kick-start a bottom-up push for change.

The Transformation Chairs Network has gone through several "transformational changes" of its own. OFT's original approach was to seed the major educational institutions within the Department of Defense (DOD) with experts who would then facilitate curriculum changes supportive of transformational thinking. To create incentives for the various schools, DOD provided funding for 3 years to cover the experts' costs and support student research. After the 3-year period, each institution was to decide on the worth of the chair position and whether to continue funding it. Under this program, 13 chair positions were formed that covered most of the intermediate and senior educational institutions within DOD, as well as the Service academies. The group met quarterly, and most meetings revolved around the challenges in establishing the legitimacy of the chair position, creating viable curricula for the schools, and pressing the fundamental concepts of transformational change. The program was vibrant, and the network quickly coalesced into a strong, collaborative organization.

The first serious challenge, and the opening of the second phase for the transformation chairs, was bridging the funding gap when DOD funding ended and the individual institutions had to assume the cost of the program. The group did shrink but stayed surprisingly strong and larger than many had expected. In addition, international players, recognizing the importance of transformation and interested in tapping into the U.S. initiative, started joining the group. By mid-2009 Australia, Singapore, Sweden, and the UK were represented. The quarterly meetings changed in character and substance, moving away from the more mundane administrative and curricula issues and into

substantive debate over the critical challenges rapid change was creating for the military. Introduction of international views greatly expanded the discussions and broadened the expertise within the group. Quarterly meetings were now combined with a lead-in conference that brought in many outside players interested in critical issues of challenge and change. Following the conference, the network would meet and continue the debates and plan activities for the future. Efforts moved from concepts to action with the addition of conferences, the publication of monographs, and direct support of DOD initiatives. For example, during 2008–2009, efforts by network members were instrumental in increasing the emphasis placed on the teaching of cyber-related issues in the Officer Professional Military Education Policy issued by the Chairman of the Joint Chiefs of Staff.

The third phase for the Transformation Chairs Network started with the first International Transformation Conference held in Stockholm, Sweden in June 2009. The theme of the conference was *Crosscutting issues in Transformation: Interactions and Innovations among People, Organizations, Process, and Technology.* Thirteen papers were presented and are published in this volume. Following the conference, the transformation chairs agreed on an expanded venue for the network, solidifying the international nature of the program and formally adopting a new direction for the group captured by the mission and vision statements cited above. Links also were tightened with NATO's Allied Command Operations and Allied Command Transformation.

The goals of the International Transformation Chairs Network are to:

- inform ongoing debate with forward-thinking concepts on major transformational issues,
- conduct research that identifies crosscutting issues, opens new vistas, and validates (or challenges) current initiatives,, and
- shape and share curricula to help educate and prepare future leaders and decision-makers.

Essay 1

Transformation—An Assessment

By Grant Hammond

Introduction

For over 15 years now, the U.S. military and numerous North Atlantic Treaty Organization (NATO) allies and other nations in the West have been committed to a process called "transformation." Born of the "Military Technological Revolution" of Marshall Ogarkov,[1] morphed into the Revolution in Military Affairs forecast by the U.S. Joint Vision 2010,[2] and institutionalized in the formation of the Office of Transformation in the Pentagon and Allied Command Transformation in NATO, it is a complex process more evolutionary than revolutionary. As Andrew Marshall of the Office of Net Assessment in the Pentagon explained, there really is no revolution in military affairs—no transformation—until the new technologies have been incorporated into changed processes, organization, and doctrine, and this takes time.[3] There were two main schools of thought regarding transformation. One saw it as the Revolution in Military Affairs, another saw it as the challenge to cope with the changing security environment of the 21st century.[4] The meaning of the term *transformation*, other than as a substitute for *change*, has been unclear. The term has meant different things to different countries, services,

---

[1] See Dale Herspring, "Nikolay Ogarkov and the Scientific-Technical Revolution in Soviet Military Affairs," *Comparative Strategy*, 1987;6(1):29–59.

[2] *Joint Vision 2010* (Washington, DC: Office of the Joint Chiefs of Staff, 1996).

[3] One of the better articles is by Ian Roxborough, "From Revolution to Transformation: the State of the Field," *Joint Force Quarterly*, 2002; Autumn:68–75.

[4] See Martin van Creveld, *The Transformation of War* (New York: Free Press, 1991).

organizations, and individuals. This has been understandable, given the different circumstances of all those who have embraced the concept and enshrined the process. As we have been reminded many times, "transformation is a journey, not a destination," and so it may be—but this means there may be no agreed-on vision, explicit goals, or consistent definition in the effort.

There are at least three different meanings contained in the term *transform*. One is change in the outward form or appearance of something or someone. In acquiring new equipment, many a nation has "transformed" and has modernized the force and acquired new capabilities. A second meaning is a deeper, more complex notion implying a change in the condition, nature, or function—a conversion into something else. In "transforming," many NATO allies hoped to be able to participate in, if not genuinely become, a modern, net-enabled force that could be interoperable with the United States and other major NATO allies. A third meaning is to change the personality or character of an entity. This is a much more complex process, but an essential one if we are to cope with the challenges of the 21st century.

Most militaries have focused on the first meaning and equated it essentially with modernization, particularly of communications, command and control, and various improvements in hardware. They have focused on the technological aspect of transformation. Others have seized on the term and the process to rationalize (in both senses of the term) the need to downsize their militaries and reorganize them into smaller, supposedly more capable, forces. For many, transformation meant changing from a conscript to a professional military. Great effort has been expended in changing organizations, processes, and military doctrine for a transformed force. Far less attention has been paid to the third meaning of the term—the change in personality or character of those who constitute the military. I contend that the essence of a successful transformation requires a fundamental change in the attitude, as well as aptitude, of those who make up the uniformed military and their political masters. We must learn to think differently and to educate and train ourselves to adapt. One of NATO's two strategic commands is Allied Command Transformation (ACT) in Norfolk, Virginia. Its vision statement is, "ACT will be NATO's leading agent for change; enabling, facilitating and advocating continuous improvement of military capabilities to enhance the military interoperability, relevance and effectiveness of the Alliance." Its strategic objectives are to provide appropriate support to NATO

missions and operations; lead NATO military transformation; and improve relationships, interaction, and practical cooperation with partners, nations, and international organizations.[5] As a major effort of the world's most successful collective defense organization, these are worthy goals and vision, but they are not very specific in content. Change and continuous improvement are important, but accomplishing their implementation is difficult.

Transformation and the Transformed World

There are several reasons that this implementation is challenging. The first is that the world in which we live has been transformed in all three of ways discussed above—outward form and appearance, condition and nature, and the character of those who act in it. Monolithic, state-centric, conventional military threats of the 20th century have largely given way to a world of insurgencies in failed and failing states and the rise of non-state actors in a globalized world of complex interdependencies in an expanded contest of irregular warfare. States no longer have a monopoly on knowledge, resources, and power; these are now obtainable to some degree on the Internet and accessible with a laptop and a credit card—both of which can be stolen. Second, the very nature of security has been transformed, certainly after 9/11, if not before. Security—protecting citizens and territory—now is no longer solely the province of the state and the uniformed military. It has become personal, municipal, corporate, and cyber, as well as national, regional, and international. It is economic and social, not merely political and military, and the number of private military companies, the instances of piracy (both naval and intellectual), and the tens of thousands of gated communities in which many well-to-do people now live all testify to the declining capability of the state to provide security. Third, the actors and what motivates them are no longer groups of citizens of states but, rather, Internet-connected groups of "netizens"— those who owe allegiance to or are committed to serving not states but innumerable causes of all kinds, particularly religious, social, and political. Individuals now have the ability to do significant harm to large numbers of people in a world in which the democratization of technology has empowered anyone or any group who seeks to combine the ability, intent, and opportunity to do harm.

---

[5] Allied Command Transformation homepage at http://www.act.nato.int/content.asp?pageid=200 [Accessed April 17, 2009].

In using the term transformation, a more imposing term for the more pedestrian word "change," we are right in suggesting that this is a complex process and ultimately something more than replacing one thing with another. However, we also miss some of the implications of the process of change. Rolf Smith wrote an interesting little book[6] a number of years ago in which he suggested there were seven levels of change. These were:

1. Do things right—being efficient.
2. Do the right things—being effective.
3. Copy what others have done—being smart.
4. Do what nobody has done—being novel.
5. Do things differently—being creative.
6. Do what should be done—being moral.
7. Do what cannot be done—being truly successful.

Each level increases in difficulty, but true change, a genuine transformation, is only achieved at level seven. We need to pay attention to all levels but accept that we may only accomplish one at a time. In attempting to change—to transform—we must keep the totality of the effort in focus and accept that priorities may change through time and circumstance. That said, ultimately it is peoples' perceptions that matter most, and how individuals come to view the process, support the vision, and nurture the process is the key to success. In embracing the process of transformation, we have done well at levels one through three and made reasonable progress in levels four and five. We have done less well on the heart of the matter—levels six and seven.

In short, transformation ought to be about not just how we do things—which has been the bulk of the emphasis to date—but what we do and why. Chris Coker's new book, *War in an Age of Risk*,[7] argues forcefully that war is no longer about a battle of wills but is instead an exercise in risk management. We live in an era in which it is far more difficult to protect the citizen than to protect the state, but in democratic societies, the citizens are the state, and public opinion constitutes the ultimate center of gravity. This is true in any conflict in which democratic societies contend—economic competition in the marketplace, political debates in the corridors of power, or war,

---

[6] Rolf Smith, *The Seven Levels of Change* (Houston, TX: Tapestry, 2009). The book was originally published in 1997; a third edition has just been published.

[7] Christopher Coker, *War in an Age of Risk* (Cambridge: Polity, 2009).

whether conventional or irregular. It becomes even more important in unrestricted warfare, such as that described by the Chinese colonels a decade ago.[8] They saw a world in which there was a contest in several arenas, as illustrated in the table below defining three groups of warfare.

Military	Transmilitary	Nonmilitary
Atomic	Diplomatic	Financial
Conventional	Network	Trade
Biochemical	Intelligence	Resources
Ecological	Psychological	Economic aid
Space	Tactical	Regulatory
Electronic	Smuggling	Sanction
Guerrilla	Drug	Media
Terrorist	Virtual (deterrence)	Ideological

Looking at war in this manner redefines the battle space and the time, the matter, and the energy required to compete successfully. If, as Coker suggests, war is now an exercise in risk management, managing the totality of these risks is hugely complex, and much of it is not the responsibility of the uniformed military. Instead, it is a task incumbent on us all in our various roles—as parent, citizen, consumer, or investor. It is also an example of the sort of transformation that is most important—transformation in how one thinks and perceives the security challenges and the environment in which one competes. Perception informs behavior, and thinking changes one's perceptions. How we identify, define, and think we must respond to the security environment around us is crucial if we are to survive and prosper in it.

---

[8] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, February 1999). The table is in chapter 5, "New Methodology of War Games," in the section entitled "Using Addition to Win the Game." This is translated by the Foreign Broadcast Information Service and is available zipped at http://cryptome.org/cuw.zip [Accessed May 20, 2009].

Future Studies

The U.S. military in particular has specialized in the last decade and a half in trying to envision the world of the future. It was a necessary task to think about how the world might evolve in the aftermath of the Cold War. The planning that has taken place has been necessary, and the futures the military has explored have been useful, but the planning has provided only instrumental goals. These goals are vehicles to help us learn to think about the future, not necessarily blueprints for it. If done well, they can narrow the aperture of risk, or at least help get a sense of the balance or imbalance of risks and responsibilities. The latest example of a major effort of this sort is the ACT study, the *Multiple Futures Project*.[9] A year-long study on the future and its implications for NATO, the project is a broadly gauged comprehensive look at the possible emerging security landscapes of the future and the organizational, technological, and procedural implications for the Alliance as a result of these trends and their implications. It was an ambitious study and a major accomplishment for ACT that will serve to educate the member nations regarding the challenges they will likely face in the future and the large list of things the Alliance will have to do to cope effectively with them.

Such studies, valuable as they are in attempting to anticipate, prepare for, and shape the future, are of limited use as plans for the future. This is because the future is a world populated by the likes of Ambrose Bierce, Yogi Berra, and black swans. Ambrose Bierce defined a plan as the best means of accomplishing an accidental result.[10] Yogi Berra's famous remark that "it's tough to make predictions, especially about the future"[11] rings true, despite the unintended humor. Nassim Taleb has written about the occurrence of the highly improbable "black swan" event, which is unpredictable, has

---

[9] Allied Command Transformation, *Multiple Futures Project: Navigating Towards 2030*, May 2009, available at http://www.act.nato.int/ MultipleFutures/ [Accessed May 8, 2009].

[10] Ambrose Bierce, *The Devil's Dictionary*. These cynical definitions were collected and published by Bierce (but never copyrighted) in 1906 and 1911. A compilation of these definitions is available at http://www.thedevilsdictionary.com/?P [Accessed April 20, 2009].

[11] Quotation available at http://www.dictionary-quotes.com/it-s-tough-to-make-predictions-especially-about-the-future-yogi-berra/ [Accessed April 20, 2009].

a massive effect, and for which we concoct an explanation that makes it seem less random after the fact.[12] All swans were thought to be white until Australia was discovered and found to have black swans. History moves not as a smoothly flowing river but resembles more what paleontologists call "punctuated equilibrium,"[13] in which random occurrences move evolution along a different path. Constantine's conversion to Christianity, the Black Death in medieval Europe, the Great Depression, and the events of 9/11 were all "black swans" of immense impact for the world. Though seen as possible and plausible in hindsight, they were not predicted, and their consequences and how to deal with them were largely unplanned.

Things get even worse. As Antulio Echevarria explains in his discussion of the proper use of history in professional military education, even though we have a record of things said and done in the past, it is only a partial record.[14] There is no such thing as objective history, for we do not have the full account from all perspectives of any event. The motivation for human action and interaction is so multifaceted that interpreting the past, however stringent the attempt at objectivity, is fraught with difficulty. There are, in effect, as many interpretations of the past as there are historians to interpret it. Although some are "better" than others, according to a particular standard or bias, there is no such thing as a perfect history of the past. We use history properly, not as vicarious experience but as an instrumental means to learn how to think better about our present and our future. Now, if this is true about the past—a string of events about which we have some, and in many cases a great deal, of certainty, if not perfect knowledge—what of the even more difficult task of interpreting

---

[12] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2008).

[13] The concept of punctuated equilibrium was a seemingly radical new idea when it was first proposed by Stephen Jay Gould and Niles Eldridge in 1972. Now it is seen as a useful model for one kind of evolutionary change. The relative importance of punctuated and gradual patterns of evolution is a subject of debate, but the concept serves as a useful metaphor in looking at the course of human history in which large-scale change appears seemingly randomly amid a slower pace of change. However improbable some of these mutations may have been, some have had an enormous effect on the evolutionary process.

[14] Antulio J. Echevarria II, "The Trouble with History," *Parameters*, Summer 2005, 78–90.

the future? Here we have no record of things said or done, yet we attempt to tell the story of our future. It is immensely difficult. Broad brush strokes can be placed on the canvas of the future, but the image resembles at most an exercise in impressionist painting, not photorealism. We should not imbue such efforts with more precision than they deserve.

The implications of this reality were captured by Secretary of Defense Rumsfeld when addressing a group of airmen at Andrews Air Force Base in 2001 (before the events of 9/11). He stated, "Your task is to defend your nation against the unknown, the uncertain, the unseen and the unexpected."[15] This of course is both absolutely correct on one level and impossible on another. It is the nature of the future that it is a landscape populated with unknowns. It is also the case that we must attempt to meet the challenges that these unknowns may present, and although we may think about what may transpire and how we might better cope with certain eventualities, we are unlikely to consider all the possibilities or prepare adequately for them. We can, however, try to shape things as best we can and prepare ourselves to be innovative and adaptive as the need arises.

Tradition versus Adaptation

The American military (and one suspects a great many others that have emulated it and its practices, as well as those from whom we inherited these practices) is ill prepared to contend with these challenges. The reasons—and remedies—have been explained by Donald Vandergriff in a number of books and studies he has conducted.[16] The military decision-making process was created in 1897

---

[15] *American Forces Press Service*, "Rumsfeld Says US Forces Building 21st Century Military," speech given at Andrews AFB, MAY 21, 2001, available at http://www.defenselink.mil/news/newsarticle.aspx?id=45841 [Accessed May 20, 2009].

[16] Donald E. Vandergriff was known as "the most influential Major in the Army" before his retirement in 2005. These ideas were first presented in unpublished forms as "From Swift to Swiss: Tactical Decision Games and Their Place in a Reformed Military Education," January 2005, and "Military Education—We Are Stuck in the Past," January 13, 2005. He has developed an approach to education and training called the Adaptive Leadership Methodology that has been very favorably received. He is the author of three books: *Path to Victory: America's Army and the Revolution in Human Affairs* (Novato, CA: Presidio, 2002); *Raising the Bar: Creating and Nurturing*

and is based on a misreading of German military training in the 19th century wedded to the ideas of Frederick Taylor to create a systematic, checklist approach to problem solving that has evolved but is largely the same today. As Vandergriff explains it, both the French and the Americans misinterpreted what the Germans had done and why they had done it in educating and training their officer corps. The Germans, he maintains, were teaching their officers how to think, not what to think, through the use of tactical decision games. The Prussians, and later the Germans, used these games to confront officers with the unknown and improve their decision-making skills. However, America adopted what it thought were the rules and procedures of the German training process and molded them as a tool for military planning. Both the five-paragraph field order and the task, condition, and standard approach to task training were based on a mistaken appreciation for German training techniques. These techniques served America well in the past because they were developed for a mass conscript Army that would need to be mobilized and trained quickly, not the all-volunteer professional force that we have today. What is required now is the much deeper and better education and training of military professionals who will execute the missions, not train others to do so in large numbers. What emerged was a near catechetical approach to doctrine with little room for the need for adaptability. Vandergriff has done much to champion the adaptive learning method and promote a review of the personnel system for the U.S. military in general and the U.S. Army in particular.

It is in the mental preparation for how to cope with ambiguity that we can address mental transformation and invest in teaching people how to cope with unexpected change. People can be taught to think conceptually, critically, and creatively and to cope with the unknown, uncertain, unseen, and unexpected, but doing so requires mental preparation. There are many suggestions for how to do this.[17] Most

---

Adaptability to Deal with the Changing Face of War (Washington, DC: Center for Defense Information, 2006); and *Military Recruiting: Finding and Preparing Future Soldiers* (Greenwood, CT: Praeger, 2008).

[17] Among many possibilities are Michael Michalko, *Thinkertoys: A Handbook for Creative Thinking Techniques* (New York: Ten Speed Press, 2004); Peter Senge's *Fifth Discipline* and *Fifth Discipline Fieldbook* (New York: Doubleday, 1990 and 1994, respectively), and his notion of a learning organization and its requirements; and works on decision-making by Gary Klein: *Sources of Power: How People Make Decisions* (Cambridge, MA: MIT

important, however, is the development of a cast of mind—a habit of thought that sees the uncertain and unknown as an opportunity, not a threat. One learns to be comfortable with ambiguity, which is a requirement for living in an era of exponential change on a variety of levels. Yet nowhere in the *Multiple Futures Project* or most other future studies will you find anything about the central element of the problem—learning how to think about how to live in a world of increasingly fast-paced, complex, uncertain, and largely unknowable change. We can surround ourselves with all kinds of technological advances to accomplish numerous tasks faster, better, and cheaper than we do now, and we can organize to take advantage of these capabilities and processes to maximize efficiency and effectiveness, but if we do not prepare ourselves for how to think and cope in this world, we will not have made the fundamental transformation that is required.

So, how should we come to think about the future? Is a change in outlook, attitude, and how we perceive change necessary to coping with our headlong rush into the future? I think it is, and it begins with a dose of humility. For all our accomplishments as human beings, and the imprint we have made on the planet for good and ill, we still know little about many of the basics of life and life-forms, of climate and climate change, of the interconnected nature of the species of flora and fauna with whom we share the earth, or the vagaries of chance and the twists and turns of human nature. Nor are we omnicompetent in our knowledge of other people, cultures, histories, and places. However much we do know, it is dwarfed by the immense amount of things that we do not know and those things that, at the moment at least, we cannot know. In this sense, ignorance is bliss, for we do not know what we do not know, and how important it might be. All this is true of our present reality. It becomes much more abstract and complex in contemplating the future and the essential nonlinearity of our predicaments. The only way to cope effectively is to learn to cope with ambiguity, to coevolve with a constantly changing environment and adapt effectively with changing circumstances as best we can. Being able to do this should not be left to chance. Rather, we should engage in the mental preparation that will help us do this.

Adaptation is essentially the process of changing in structure, function, or form to improve chances for survival within a given

Press, 1999), and *The Power of Intuition: How to Use Your Gut Feelings to Make Better Decisions at Work*, (New York: Broadway Business, 2004).

environment. As the environment changes, one must continue to adapt to survive. If the world described by many books and future studies proves to be anywhere near the reality we will encounter, asymmetric threats, unrestricted warfare, non-state actors, global interdependence (both positive and negative), and a host of other novelties in a rapidly evolving security landscape will be the norm, and the pace of change—the number and type of "black swans" that we might encounter—could very well be different than what we have told ourselves to expect. We can and will adapt to some elements of our future, for we have a greater degree of certainty about some of them,[18] but we have less understanding of their potential consequences, processes, or events that we cannot foresee.

The U.S. Military and Planning for the Future

Consider a military planner thinking about the future in 1913. War among the great powers is to him a possibility, but not very likely because of the complex web of alliances that contributes to a balance of power, because the world is in the midst of an unprecedented era of globalization and the interdependency that implies, and because no one seems to want a war, despite some outstanding disputes. However, he could well have predicted that, should war occur, there would be a number of critical products and technologies that would play a role. Barbed wire and trench warfare, machine guns and large amounts of artillery, the use of the submarine and the airplane—all were predictable, but they were less important than the consequences that flowed from their use and the outcome of the war that followed: the Russian Revolution, the collapse of four empires, the League of Nations, the rise of communism and fascism, the Great Depression, and another war after what E. H. Carr called "the twenty year crisis."[19] Although we may do well at predicting technologies and weapons systems that may come to pass, the social, political, and economic

---

[18] Among recent reports and Web sites dealing with how to learn how to adapt and educate and train others to do so are William R. Burns, Jr., and Waldo D. Freeman, "Developing an Adaptive Training Strategy and Policy for DoD," Interim Report, Institute for Defense Analysis, October 2008 and the Web site Project White Horse, at http://www.projectwhitehorse.com/ [Accessed October 12, 2009].

[19] E. H. Carr, *The Twenty Years' Crisis, 1919-1939: An Introduction to the Study of International Relations* (New York: Harper Perennial, 1964).

dislocations that arise as a result of their use are far more difficult to anticipate. Even regarding technology, one should be chastened about predicting the future. In the early 1930s, *Fortune* magazine predicted the coming of the "electro-chemical war"—a view that was only partially correct—and *Collier's* in the 1950s foresaw colonies on the moon by 2000. It is a difficult business, preparing for the future.

That being said, preparing for the future is a necessary military task. If militaries are to function effectively in a rapidly changing world, they must learn to adapt quickly and well, and many of the officers who will make many a critical decision in 2030 (only two decades away) are already in the military of today. Are we preparing them as we should? I think not. And the irony in this circumstance is that we know what to do—we are just not doing it as well, as often, or as broadly as we need to. The U.S. Army Research Institute has done a lot of studies on adaptability, and as long ago as 2004 the institute stated in its research newsletter that, "To produce good military adaptive thinkers one must train a performance—a thinking performance—in much the same way that one trains any skilled, well-rehearsed, and extensively practiced behavior to enable expert performance."[20] The institute went on to state that, "We recognize that leadership in complex adaptive systems relies on relationship-building over role-defining, loose coupling over standardization, learning over knowing, self-synchronization over command and control, and emergent thinking over planning based on estimates." The newsletter concluded:

> A contingency-based and responsive Army must place an enduring premium on a soldier that can work at any level within the spectrum of warfare. The vision of such a soldier, and the Army to which he belongs, is one of leadership that is flexible and adaptive. These leadership traits can only become intuitive to our leaders through a system of education and training for both officers and non-commissioned officers that continues to be innovative, sequential and extensively resourced at all levels throughout the transformational Army.[21]

There, in a single paragraph, is a blueprint for all modern militaries, both the United States and NATO allies, for how best to prepare for the future. Deployments to Iraq and Afghanistan have reinforced the importance of the message. As Dr. Leonard Wong of the U.S. Army's

---

[20] "Adaptive Leaders and the IBCT—Initiative Within Intent," *ARI Newsletter*, 13(1), 2004.
[21] Ibid.

Strategic Studies Institute noted,[22] accomplishing the mission in Iraq was dependent on the ability of officers to adapt to uncertain, complex environments and novel circumstances. Army Special Forces units in particular excel in just this. To some degree, this human capability is being addressed, but not across the U.S. military, and certainly not throughout NATO.

According to the conclusions of one study, the U.S. Navy in general "has geared all of the competencies to business, to organizational development, to the application of technology, and not to warfighting." The study went on to say that, "the Navy treats leadership as a task that requires certain skills depending on the specific job or rank of the individual."[23] The same study 5 years ago found that the U.S. Air Force "was beginning to address the development of adaptability based skills; however, the Air Force must devote more initiative and resources if it wants to see the transformation it seeks."[24] The U.S. Marine Corps has long emphasized adaptability and "has incorporated adaptability-related learning across the board." Largely as a result of the effect of U.S. Air Force Colonel John R. Boyd[25] and his emphasis on maneuver warfare and teaching at the Basic Course in Quantico for a number of years after his retirement, the Marine Corps has been emphasizing adaptability for a long time. "Since war is a fluid phenomenon, its conduct requires flexibility of thought. Success depends in large part on the ability to adapt—to proactively shape changing events to our advantage as well as to react quickly to constantly changing conditions."[26] The Marines have gone farther faster in this emphasis than any of the other services and seek to make room for errors and mistakes, so as not to punish initiative by institutional prejudice. They use tactical decision games extensively to develop adaptability and cognitive skills in courses and exercises. They even publish a tactical decision game monthly in the *Marine Corps Gazette.*

---

[22] Leonard Wong, *Developing Adaptive Leaders: The Crucible Experience of Operation Iraqi Freedom* (Carlisle, PA: US Army War College, 2004).

[23] John C. F. Tillson et al., *Learning to Adapt to Asymmetric Threats,* (Washington, DC: Institute for Defense Analysis, 2005), 30.

[24] Ibid, 33.

[25] On Boyd and his effect on the U.S. military, see Grant T. Hammond, *The Mind of War: John Boyd and American Security,* (Washington, DC: Smithsonian Books, 2001). Reprints in paperback, 2004 and 2007.

[26] U.S. Marine Corps, "Warfighting," Marine Corps Doctrinal Publication 1, 1997, 17.

So, 5 years ago for some, and nearly 20 years ago for the Marines, at least some in the U.S. military knew how to solve some problems to prepare for a difficult future in educating and training its members. However, this thinking has not permeated all the services or the Office of the Secretary of Defense, nor has the general insight that trust, cohesion, and interpersonal dynamics—human interoperability—are more important than the technology used if we are to fashion effective, adaptive teams in the military. There is a certain irony here in that it is entirely likely that it is easier, faster, and cheaper to incorporate interpersonal dynamics than to assimilate new technologies and all their supporting doctrine, process, and organizational structures—things that the U.S. military seems to specialize in doing. As long as DOD in particular, and the U.S. military (and NATO allies and partners in varying degrees) in general, are committed to hierarchical control, centralized established policies, and micromanagement to ensure compliance to a standard, progress is likely to be slow and ineffective.

Transformational Thinking

What, then, are the requirements for educating and training for adaptability? Let me enumerate them as I have come to think of them based on a large amount of reading and analysis from a variety of sources. These are not unique and are not my ideas only. They are the compilation of a host of insights, both general and specific, from some 20 years of working in professional military education and are offered as one perspective on transformational thinking, which I consider to be the essence of the process.

There is no substitute for the basics—for not just knowing but understanding and being able to demonstrate how to use the facts one needs to know, the basic skills of one's profession (e.g., military occupational skills for the U.S. Army, Air Force Specialty Code for the U.S. Air Force). Whether small unit infantry leader or pilot, one needs to know thoroughly the basics and understand how these contribute to mission effectiveness. However, it is more than reciting a checklist or the platoon leader's warning order, it is understanding how to use them and being able to do so. This is thought of as training (giving answers to "How?") but is actually education as well (asking both the "What?" and the "Why?" questions to better understand). Thorough knowledge and understanding at this level are essential to everything else and cannot be diluted, waived, or sacrificed in any way.

Develop a sense of self-awareness and self-knowledge and build a team. You must come to know yourself—your strengths and weaknesses—if you are to maximize the talents of the team you will be a part of or the group you intend to lead. Not knowing yourself means you cannot fully exploit the capabilities of others and maximize their contribution—and yours—to the task at hand. It is the essential bedrock for establishing solid interpersonal dynamics and relations, to build the human interoperability that is essential for groups—joint, interagency, and especially multinational. If you do not know yourself and only endeavor to know others, you know only half of what is required to form an effective team. By knowing others well, you can begin to know what must be done to build a team and sustain the cohesion and commitment necessary for military units to perform well.

Know what to know about others, especially those with whom you must work. You must come to understand those in your command, particularly those under your command, and how best to work with them. This requires good powers of observation, objectivity, a dose of empathy to see things from another's perspective, and a broader understanding of individuals and the groups to which they belong. At base, you must know the following about those who are under your command, those who are allies, those who are adversaries, and those who are merely observers: What do they value? What do they fear? What motivates them? What is their purpose (short-term and long-term)? If you can answer these questions, you can build an effective strategy to interact appropriately with any group, whether to cooperate, contend, deter, defeat, or inform. If you do not know these things, you may have perfect knowledge in other realms (order of battle, etc.) and still fail in your efforts to interact effectively. On one level this is personal insight, biography, or a psychological profile. On another it is cultural anthropology and ethnography and an understanding of one's culture and society. Both are important.

Have the right thinking skills—conceptual, critical, and creative. One needs to be able to think theoretically and conceptually about what is going on and to have a sense of origins and precedents on the one hand and consequences, both intended and unintended, on the other. One needs to be able to analyze critically the circumstances confronting one and to devise the ends, ways, and means to deal effectively with them. However, one also needs to be able to synthesize, to be innovative and creative in finding new perspectives, approaches, and combinations to solve the problems confronted. One should be

encouraged to learn about how the decisions are made, not just what they are. This requires a combination of skills that John Boyd briefed as insight, imagination, and innovation.

Ambiguity is a permanent condition and demands risk tolerance. Most militaries select and promote those who are risk averse; those who advance do so because they have not made mistakes. Not making mistakes becomes a goal, and hence bold initiatives or risky ventures are avoided as endangering one's career. Officers should be encouraged to explore novelty and nonlinearity and to risk making mistakes without being punished for displaying initiative. Commanders should encourage experimentation, acknowledge that failure is a possibility, and not penalize those who fail because they are learning how to be intuitive and innovative. Learning how to cope with ambiguity and treat it as an opportunity and not a threat means taking risks, making mistakes, and learning from them. Over time, success in learning how to cope with ambiguity will help develop an intuition about what to do and how to do it.

Dynamic scenarios should be used in which all of these skills need to be exercised frequently under a variety of conditions and tasks. Officers should be continuously faced with novel circumstances that cause them to have to adapt to new situations. Rather than command- or contractor-scripted war games whose outcome is known in advance (blue always wins), or short tabletop exercises with school solutions, one should use dynamic scenarios, both in the classroom and in the field. These scenarios should occur over 3 days or so and call for a series of decisions based on a flow of events over time that continually confront those involved with dynamic circumstances and novel challenges for which they are not prepared. Such dynamic scenarios are in effect carefully designed decision-making exercises to teach people how to become intuitive and adaptive. Participants should have to confront the unintended consequences of their choices and contend with the implications as a way to learn. They should never be allowed to get comfortable with a routine set of tasks. This means training toward a level of competence and capability based on intuition and skilled judgment that these exercises develop and reinforce.

Red team as the adversary. The enemy is a skilled actor in his own right and is capable of making decisions to cope with a variety of realities that you may present. Conflict and war are interactive processes, and one must never forget that the opponent has an array of alternative courses of action. If one never thinks about how an

opponent may respond, or the actions and reactions that constitute his decision-making matrix, then one cannot be assured of having selected the best of one's own courses of action. The opponent has his own campaign plan and end-state in mind, and it is different from yours. You know yours—you need to know his. If you do not, or at least have not thought through the possibilities, failure becomes more likely. The enemy decides, if he is defeated, when and how and what he will do thereafter. All are important considerations.

After-action assessments are a mandatory part of the process and constitute a part of the lessons learned for groups and individuals. Experience in such contexts can be fleeting unless objectively assessed and the results—good, bad, and ugly—shared with those involved in a brutally honest way by those observing and assessing the activity. This requires a trained staff of assessors, a means for capturing and disseminating lessons, and follow-up to ensure that these become lessons learned, not lessons merely identified. It should be every bit as pointed and important as any other combat exercise and assess the thinking, decision-making, intuition, and skilled judgment—or lack thereof—of the participants. Feedback and further education and training based on that feedback to attain ever-higher skill levels is a must.

Conclusions

Gary Klein, a well-known and often-cited specialist in decision-making, identified those traits that inhibited adaptability in teams: training for mastery of routines; telling people what to think, not teaching them how to think; focusing on the accomplishment of a plan, which will not likely survive first contact with the enemy, who is a thinking actor in his own right; using rigid and centralized command and control based on ever-greater amounts of information; and reliance on increasingly detailed and directive plans that are difficult to change.[27] Yet we have persisted in creating military staffs at both the operational and strategic level that handle "planning" at ever-higher levels of detail, often resulting in lower levels of accomplishment. Myriad matrices, tables, annexes, acronyms, and templates purport to explain alternative courses of action, campaign plans, and directives to subordinate units, increasingly with massive amounts of data fusion, in

---

[27] Gary Klein, *Adaptive Teams: Final Report* (Fairborn, OH: Klein Associates, 2001), 1–27.

which intelligence, maps, and overhead imagery are combined to give a better picture of the battle space. However, command and control by plan rarely resembles the reality one encounters. True, certain elements—scheduling, logistics, and so on—demand extraordinary amounts of precision, but it should be more about what John Boyd called "appreciation and leadership" than command and control.

We substitute data for information and assume that information is knowledge, knowledge is wisdom, and wisdom is truth. Alas, this is frequently not the case. One of the perils of the data-fused world of the commander is that he loses focus on his ultimate target—the perception of his opponent. Wars are begun, fought, and ended in the minds of men. What they make of a circumstance, what compels them to behave as they do, and their perception and understanding of the world about them—and by extension, our knowledge of their perceptions—are critical to contending with those who oppose us in a variety of contexts. Although knowing how an opponent views us and the world may be difficult to ascertain, knowing the enemy—what he thinks and why—is central to strategic engagement with him.

It is often said that transformation is a process to change an organizational culture. Culture is ultimately shorthand for people and changing how people think and behave. Culture implies intellect, mindsets, tastes, and manners, and the refinement of these by education and training. If we fail to transform how we think and act, we will not have transformed ourselves, our organizations, or our processes. Adoption of technology alone does not constitute transformation, for it is a part of the accelerating change in the world of the 21st century with which we must learn to cope.

We have had a revolution in security affairs, if not one in military affairs. The nature of security and the threats to it have changed radically. We need a revolution in military education if we are to truly transform. That revolution would abandon many of the hallmarks of military culture—centralized, hierarchical, standardized, competitive, prescriptive, sequential organizational frameworks and routines—and substitute those that are increasingly decentralized, distributed, diversified, collaborative, adaptive, and concurrent. Modern militaries, if they are to transform, must create learning organizations by recruiting, promoting, educating, sustaining, and reinforcing the ideas of people who are adaptive, intuitive, risk-tolerant, and comfortable with ambiguity. It means abandoning the traditional way in which we educate based on rote memorization, sequential performance of tasks,

and holding time constant in education and training and letting the performance vary in a system that is authority driven, hierarchically organized, centralized, and handles large numbers. This was a system designed for a 19th-century, assembly-line society and economy that no longer exist. It is on-site and on command, costly to sustain, and produces variable quality. It needs to be off-site as well as on, on demand as well as on command, customized, continuous, interactive, cheaper, and held to a high quality standard. We need to invest in teaching people how to think well and quickly, to teach them to be adaptive and synthetic as well as analytic in their thinking, and to imbue them with a form of intellectual *Auftragstaktik*. Our minds are our best weapons and a force multiplier. We should spend as much time, care, and attention on them as we do on the equipment we are issued and value thinking as much as doing. All are difficult for military cultures.

Until we start to think differently, to learn how to think differently and to learn how to cope with ambiguity, to adapt and to contend with a complex, uncertain, rapidly evolving future, we will not really have reached the seventh level of change. We will not have transformed. Doing so in a world of "inevitable surprises" is a necessity. As Peter Schwartz has counseled, "Place a very, very high premium on learning. Most failures to adapt are, in effect, failures to learn enough in time about the changing circumstances."[28] Relative to the cost and effect of other kinds of transformation, investments in transformational thinking would seem to be far less expensive and pay greater dividends. It is time we got started in earnest and do more than pay lip service to the concept.

---

[28] Peter Schwartz, *Inevitable Surprises: Thinking Ahead in Times of Turbulence*, (New York: Gotham Books, 2003), 233–234.

A Conceptual Framework for Innovation in Capability Development

By John J. Garstka

Abstract

This essay examines the different types of innovation carried out by military and civilian organizations and the factors that can influence an organization's ability to innovate, which is a function of both individual and organizational behavior. Perspectives on innovation from multiple domains can be synthesized to develop and refine insights into the factors that influence the ability of military organizations to innovate in developing and enhancing capabilities.

Introduction

There is wide consensus that organizations need to be able to successfully innovate to deal with challenges and exploit opportunities. Governments are often forced to innovate to meet the challenges posed by unforeseen crises, such as the September 11, 2001, terrorist attacks, the outbreak of SARS in 2003, and the international financial crisis of 2008–2009. Militaries and defense organizations innovate in the development of strategy and in the development and employment of forces. The challenges faced by defense organizations can take the form of increased belligerence of a nation-state or non-state actors, an adversary's development of more advanced warfighting capabilities, a deteriorating budget environment, or imposed requirements, as is the case for the nations looking to join NATO. In the commercial sector, innovation is focused on products and services. Challenges faced by commercial organizations include deteriorating economic conditions, actions of a competitor, changing consumer preferences, and shortcomings in leadership or management. Examples of opportunities in the commercial sector include the opening

of new markets, technology breakthroughs, the misstep of a competitor, changing consumer preferences, and a change in regulatory structure.

Perspectives on Military Innovation

Military organizations need to be able to innovate successfully to develop and sustain competitive advantage. Militaries that have failed to innovate have often suffered at the hands of competitors who have more effectively developed and employed new warfighting abilities. Developing new concepts and translating them to operational capabilities requires military organizations to be able to innovate in a range of areas and on different time scales.

Scholars have identified both macrolevel and microlevel factors that can contribute to, or attenuate, the ability of military organizations to innovate. These include civil–military competition (Posen, 1991), interservice competition (Cote, 1996), intraservice competition (Rosen, 1991; Posen, 1991), the role of organizational culture (Kier, 1997; Murray, 1996), and the importance of unmet military challenges (Hundley, 1996).

Posen asserts that a state's security environment can create a demand function for innovation. States react in rational ways to address insecurities by either acquiring allies (addressing the external balance) or strengthening their militaries (addressing the internal balance).[1]

Stephen Rosen categorizes innovations as either major military innovations or technological innovations.[2] Major military innovations change organizational behavior, resulting in either the creation of a new arm of a service or changes in how one of the major combat arms of a service fights. Rosen also highlights the important role played by both product champions and viable career paths in enabling the development of new warfighting capabilities.

Cote concludes that innovation is influenced to a large degree by intense competition between services.[3] Examples of where interservice competition played a role include the competition between the U.S.

---

[1] Barry Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, NY: Cornel1 University Press, 1991), 13–33.

[2] Stephen Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornel1 University Press, 1991), 1–53.

[3] Owen Cote, "The Politics of Innovative Military Doctrine: The US Navy and Fleet Ballistic Missiles," PhD Thesis, MIT (January 1996).

Army and U.S. Navy in the development of military aviation and the competition between the U.S. Air Force and the U.S. Navy associated with the development of ground-based intercontinental ballistic missiles and submarine-launched ballistic missiles.

Kier posits that a state's choices in developing doctrine are shaped by cultural factors.[4] She found that organizational culture can predispose an organization to offensive military operations or defensive military operations and can also shape the trajectory of innovation that militaries pursue. Murray highlights the importance of organizational culture in creating a climate that is open and supportive of innovation and experimentation.[5]

Hundley highlights the importance of unmet military challenges in creating a demand for new warfighting capabilities in revolutions in military affairs. He identifies the importance of combining doctrinal and organizational change with technology innovation, as well as the key role played by operational concepts. He also highlights the importance of institutional processes for exploring, testing, and refining conceptions of future war—that is, conducting experiments and assessing their results in facilitating the innovation associated with revolutions in military affairs.[6]

Each of these perspectives describes key factors that enhanced or constrained the ability of military organizations to innovate in the context of various operational and strategic contexts. Insights into organizational innovation in the commercial sector can shed light on additional factors that can influence the ability of military organizations to innovate.

Insights Relating to Innovation in the Commercial Sector

Innovation in the commercial sector primarily revolves around the development of products and the offering of services. This primary dimension of innovation is supported by five other types of innovation.

---

[4] Elizabeth Kier, *Imagining War: French and British Military Doctrine Between the Wars* (Princeton, NJ: Princeton University Press, 1997), 144–145.

[5] Williamson Murray and Allan R. Millett, *Military Innovation in the Interwar Period* (Cambridge, UK: Cambridge University Press, 1996), 312–318.

[6] Richard Hundley, *Past Revolutions, Future Transformations* (Santa Monica, CA: RAND Corporation, 1996), xiii–xxiv.

- Product and service innovation involves the introduction of substantially improved goods and services. Innovations of this type might include improvements in function, characteristics, or technical abilities.[7]
- Process innovation involves the implementation of a new or significantly improved production or delivery method.[8]
- Marketing innovation is the development of new marketing methods with improvements in product design or packaging, or the promotion or pricing of products or services.[9]
- Organizational or people innovation (also referred to as social innovation) involves the creation of new organizations, business practices, ways of running organizations, or organizational behavior.[10]
- Business model innovation involves changing the way business is done in terms of capturing value. [11]

Innovation Frameworks

H.J. Leavitt, in analyzing organizational change, introduced a model of organizations that consisted of the variables of task, structure, technology, and actors.[12] Tasks were defined as the activities involved in the production of goods and services. Actors were defined to consist primarily of people, with the qualification that acts executed by people might at some time be automated. Technology was defined as problem-solving interventions such as computers or production machinery. Structure was defined to include systems of communication, systems of authority (or other roles), and systems of workflow. One of Leavitt's key observations was that these four variables were linked and that in many situations, change in one variable would necessitate changes in one or more of the other three variables. The relationship between these variables is portrayed as a diamond (see figure 1).

---

[7] Sanjiva Dubey, *Innovation with IT* (New Delhi: Tata McGraw Hill, 2009), 5.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] H.J. Leavitt, "Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches," in *Handbook of Organizations*, edited by J.G. March (Chicago: Rand McNally, 1965), 1144–1145.
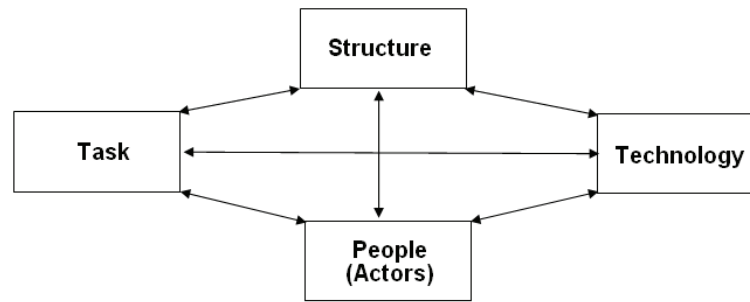
Figure 1: The Leavitt Diamond

Researchers examining how organizations employ information technology have applied constructs similar to Leavitt's. In doing so, they have focused on the relationships between information technology, process innovation, organizational structures, and the roles and skills of individuals. Initially, there was a lack of understanding with respect to the degree to which fully leveraging information technology could require changes in these three other areas.

Researchers analyzing organizations that effectively leveraged information technology to create competitive advantage identified the importance of linking strategy to information technology and organizational change. One of the more noteworthy efforts was the Management in the 1990s (MIT90s) Research Program conducted by researchers at the MIT Sloan School of Management. A key outcome of this research program is the MIT90s framework, shown in figure 2. This framework includes the elements of strategy, structure, technology, individuals and roles, and management processes, and incorporates the factors of the external technological environment and the external socioeconomic environment.[13] In this construct, structure refers to both organization and process. The MIT90s research highlighted the primary challenge in the management of transformation as managing changes in strategy, structure, technology, and people. This research effort also highlighted the importance of taking into account organizational culture when pursuing organizational

---

[13] M. Morton et al., *The Corporation of the 1990's: Information Technology and Organizational Transformation* (New York: Oxford University Press, 1991), 19–23.

transformation enabled by information technology. The MIT90s research found that organizational transformation initiatives can be significantly inhibited when changes in the area of people or organization affect organizational culture.

Contemporary approaches that address the linkage between business innovation and information technology focus on the relationships among strategy, information technology, process, and people.[14] Dubey describes process innovation as a comprehensive approach that involves innovating tasks, people, and technology for the benefit of the customer.[15]

Taken together, the Leavitt construct, the MIT90s model, and contemporary approaches clearly identify four distinct areas of innovation that are closely linked: technology, process, organization, and people. Technology and process innovation are the primary sources of competitive advantage in the marketplace, as they directly affect the development and refinement of goods and services. However, social innovations in the areas of people and organization can also be significant sources of indirect competitive advantage.

Social innovations that focus on people and organization create new means to develop, employ, and retain human capital, as well as establish or improve organizations and organizational culture. Examples of innovation in this area include labor unions and stock companies (investor-owned companies). Social innovations such as employee stock options have played a critical role in enabling startup companies to attract the human capitol they need to carry out the innovation required to develop new products and services. Social innovations are also often required to enable large organizations to develop or enhance their ability to innovate.

Types of Technology Innovation
Henderson and Clark, in their seminal paper on innovation, analyzed why firms were challenged by certain types of product innovation. They developed a framework that distinguishes between four types of technology innovation: incremental, modular, architectural, and radical:[16]

---

[14] Dubey, 76–114.

[15] Ibid., 79.

[16] Rebecca Henderson and Kim Clark, "Architectural Innovation: The Reconfiguration of Existing Product Technologies and the Failures of Established Firms," *Administrative Science Quarterly*, March 1990, 9–30.
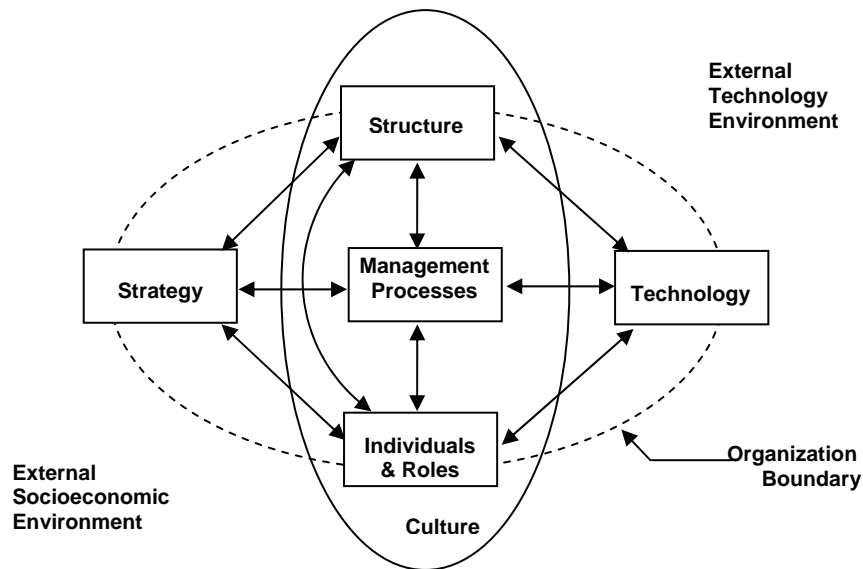
Figure 2: The MIT90s Framework

- Incremental innovation refines and extends an existing design. Improvement occurs in individual components, but the underlying core design concept and the links between components stay the same. Commercial examples include refinements to automotive car designs, the development of various models of propeller-driven commercial airliners, and refinements to cell phones.

- Modular innovation changes the core design concept of a technology. Commercial examples include the development of fuel oil-burning engines on ships to replace coal-burning steam propulsion, the development of digital phones to replace analog phones, the development of digital cameras to replace film cameras, and the shift from mechanical to fly-by-wire controls for commercial aircraft.

- Architectural innovation changes a product's architecture but leaves the components and the core design concepts they embody unchanged. Examples include the development of the laptop computer subsequent to the development of the portable computer, innovations in copier design that significantly

> reduced the size of copiers, and the creation of the Sony Walkman radio.

- Radical innovation establishes a new dominant design, and hence a new set of core design concepts embodied in components that are linked together in a new architecture. Examples include the initial development of the automobile, the vacuum tube, radio communication, the transistor, the development of the personal computer, and the development of the router.

Henderson and Clark found that firms that had succeeded in radical innovation often faltered when faced by the challenge of modular innovation. In their research, they cite the examples of the challenges posed to Xerox, the pioneer of plain paper copiers, and RCA, a pioneer in radio technology.

When competitors introduced copiers that were smaller and more reliable than Xerox's offerings, it took Xerox almost 8 years to introduce a comparable product. The missteps and false starts that occurred during this period caused Xerox to lose half its market share and resulted in serious financial problems for the company.[17] RCA faced similar challenges in the radio business when Sony introduced successive models of small transistor radios. RCA had pioneered transistor radio technology but did not believe there was a market for products built with technology they viewed as inferior to existing radios. Sony licensed the technology from RCA and gradually produced products with improved sound and FM quality that RCA could not match.[18]

Sustaining and Disruptive Innovation

Henderson and Clark observed that architectural knowledge tends to become embedded in the structure and information processing procedures of established organizations. They also observed that because of this phenomenon, architectural innovations destroy the usefulness of the architectural knowledge of existing firms while retaining the usefulness of the component knowledge. Consequently, the destruction of architectural knowledge is difficult to recognize and hard to correct. The result is that architectural innovations present

---

[17] Ibid., 10.
[18] Ibid., 10.

established organizations with subtle challenges that inhibit or preclude their ability to respond to the actions of competitors.[19]

In *The Innovator's Dilemma,* Christensen addresses the question of why firms that have a record of successful innovation can fail miserably in responding to certain types of competitive challenges. He answers this question by introducing the concepts of sustaining and disruptive innovation.[20]

Sustaining innovation creates or enhances products or services in ways that customers in mainstream markets already value. An example of sustaining innovation was Intel's innovation in the x86 family of microprocessors. The 32-bit 386 processor improved on the performance of the 16-bit 286 generation of processors, using attributes the mainstream market valued.[21]

Disruptive innovation creates an entirely new market through the introduction of a product or service whose performance is initially worse, based on the metrics valued by mainstream customers.[22] These products or services often have other features that are valued by some customers. For example, Charles Schwab's introduction of the discount brokerage was a disruptive innovation relative to the full-service offerings of brokers such as Merrill Lynch, whose mainstream customers valued the breadth of services offered by Merrill Lynch.[23]

Christensen posits that sustaining innovations over time have the potential to overshoot the performance requirements of the mainstream marketplace. Disruptive innovations are often introduced in new markets or at the entry level of existing markets. Similar to sustaining innovations, disruptive innovations gradually improve, eventually taking market share from existing products or services. This relationship is portrayed in figure 3.

---

[19] Ibid., 27–29.

[20] Clayton Christenson, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Boston, MA: Harvard Business School Press, 1997), xx–xxi.

[21] Clayton M. Christensen and Michael Overdorf, "Meeting the Challenges of Disruptive Change in Harvard Business Review on Innovation (Boston: Harvard Business School Press, 2001), 114.

[22] Clayton Christenson, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, xv.*

[23] Clayton and Overdorf, 106–109.
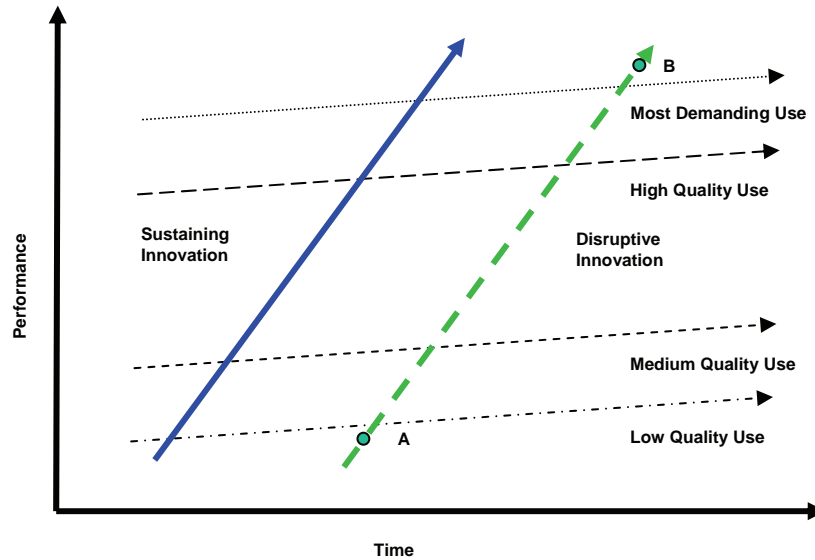
Figure 3: Performance of Sustaining versus Disruptive Innovation[24]

In providing examples of the challenge posed by disruptive innovation, Christensen describes how companies in diverse sectors have been affected by disruptive innovation. Examples of disruptive innovation by sector are portrayed in table 1.

A historic example of the effect of disruptive innovation is found in the competition between steamships and sailing ships. When steamships, a radical innovation, were first introduced in 1819, they could not compete against sailing ships in the transoceanic shipping market. In this market, steamships underperformed sailing ships in terms of speed, cost per mile, and reliability (they required frequent repair). Initially, steamships found a market on rivers and lakes, because they had a performance attribute that was highly valued: they could move against the wind or in the absence of wind (The introduction of steamship technology corresponds to point A in figure 3). Over time, steamship technology improved through sustaining innovation to the point that it could outperform sailing ship technology on the open ocean (this improvement corresponds to movement from point A to point B in figure 3).

---

[24] Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail,* xvi.

Sector	Incumbent "Technology"	Disruptive Innovation
Transportation	Sailing ship	Steamship
Construction	Cable-actuated mechanical shovels	Hydraulically actuated mechanical shovels
Financial services	Full-service brokerages	Discount brokerages
Information technology	Minicomputers	Personal computers
Steel mills	Vertically integrated steel mills	Minimills
Retailing	Full-service department stores	Discount retailers
Information technology	Unix, Windows NT	Linux

Table 1: Examples of Disruptive Innovation by Sector[25]

Despite the availability of the technology, not a single sailing ship maker built a steamship for use in any market. Their primary customers, transoceanic shippers, did not want to employ steamships until they became economically competitive. Eventually, virtually all ocean traffic was transported on steamships, and not a single company that built sailing ships survived to produce steamships in any market.[26]

In the commercial sector, disruptive innovations challenge existing organizational values or business models in a way that makes it difficult for organizations to respond. Christensen observed that companies, in an effort to grow the bottom line, tend to pursue the opportunities that they believe will best generate top-line growth. This strategy usually translates to developing products and services with higher margins for leading-edge customers in existing markets. Disruptive products appear so intermittently that almost no companies have routine processes for dealing with them. Because disruptive innovations almost always promise lower profit margins per unit sold and are not attractive to the company's best customers, they are inconsistent with the established business models and company values.[27]

In assessing the factors that contribute to an organization's ability to respond to the challenges posed by disruptive innovation, Christensen

---

[25] Ibid., xxix.
[26] Ibid., 75–76.
[27] Christensen and Overdorf, 106–109

and Overdorf highlight the relationships among an organization's resources, processes, and values. [28]

- Resources are defined as tangible assets—people, equipment, technologies, and cash—and less-tangible assets—product designs, information, brands, and relationships with suppliers, distributors, and customers.
- Processes are defined as patterns of interaction, coordination, communication, and decision-making that employees use to transform resources into products and services of greater worth.
- An organization's values are defined as the standards by which employees set priorities that enable them to judge whether an order is attractive or unattractive, whether a customer is more important or less important, whether an idea for a new product is attractive or marginal, and so on.

Christensen and Overdorf observe that as companies become large, their ability to enter new markets is diminished. This decreased capability is not caused by a lack of resources but, rather, a gradual shift in values. When an organization's capabilities reside primarily in its people, changing capabilities to address new problems is relatively simple. However, change can be extremely difficult when capabilities reside in processes and values. The difficulty of change increases significantly as processes and values become embedded in culture.[29]

Christensen and Overdorf posit that organizations have three options in developing capabilities to create new organizational capabilities for innovation:

1. create new organizations within which new processes can be developed;
2. spin out an independent organization and develop processes and values required to solve new problems; and,
3. acquire an organization whose processes and values closely match the requirements of the new task.[30]

The critical insights regarding innovation in the commercial sector discussed in this section can be summarized as follows:

---

[28] Ibid.
[29] Ibid., 113–114.
[30] Ibid., 117.

- Innovation can occur in the lines of development of people, process (task), organization, and technology.
- Innovations in one line of development often require innovations or changes in other lines of development.
- There our four types of technology innovation: incremental, modular, architectural, and radical.
- Architectural innovation can present established firms with subtle challenges.
- Innovations can be either sustaining or disruptive.
- Disruptive innovations appear so infrequently that few companies have routine process for dealing with them.
- Disruptive innovations are almost always inconsistent with an organization's established business models and values.
- An organization's capabilities for innovating are both enabled and constrained by resources, processes, and values.

Application of Insights from the Commercial Sector to Warfighting Innovation

In *Warfighting and Disruptive Technologies,* Pierce applies Henderson and Clark's innovation typology and Christensen's concept of sustaining and disruptive innovation to military innovation.[31] In doing so, he makes critical observations regarding the role of disruptive architectural innovation in explaining the success and failure of historic military innovations.

The application of the Henderson and Clark typology for technology innovation to military innovation can be illustrated by the following examples:

- Incremental innovation. This type of innovation translates to weapon and system upgrades. An example of incremental innovation is the innovation that led to the development of the Panzer IV tank after the development of the Panzer III tank.
- Modular innovation. Examples of modular innovation include the shift from analog to digital ship steering systems, the shift from coal-fired steamships to ships powered by oil, the shift

---

[31] Terry C. Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation* (London: Frank Cass, 2004), 16–17.

> from fuel oil to nuclear propulsion for ships and submarines, and the upgrade from analog radar to digital radar.
> - Radical innovation. Examples of radical innovation include the machine gun, the airplane, submarines, aircraft carriers, radar, computer-enabled codebreaking, ballistic missiles, stealth technology, and unmanned aerial vehicles.
> - Architectural innovation. Examples of architectural innovation include continuous-aim gunfire, carrier warfare, amphibious warfare, and blitzkrieg.

In applying the concept of architectural innovation to warfighting innovation, Pierce asserts that architectural innovation can take place at two levels. The first is at the system level, where components change but the system architecture stays the same. An example of innovation at the system level is continuous-aim gunfire. This innovation increased U.S. Navy gunfire hit rates by 3,000 percent. At the second level, weapons systems are defined as components, and doctrine provides the linkages between system components.[32] The product of this second level of architectural innovation will be referred to in this essay as "tactical architectures." In providing examples of architectural innovations of this type, Pierce identifies carrier warfare, amphibious warfare, and blitzkrieg.[33] Pierce then further characterizes technology innovations by applying the theory of sustaining and disruptive innovation.[34]

Sustaining military innovations improve the performance of existing systems or the prevailing warfighting architecture. Examples of sustaining innovation include continuous-aim gunfire, enhancements to battleships that increased their survivability and the range, accuracy, and firepower of their main guns, and improvements to ballistic missiles that improved range and accuracy.

Disruptive military innovations create a new source of combat power that in some way challenges or competes with the prevailing warfighting architecture of a military service. Pierce's application of the concept of disruptive architectural innovation helps to explain the underlying characteristics of a revolution in military affairs (RMA). Knox and Murray characterize RMAs as "requiring the assembly of a complex mix of tactical, organizational, doctrinal, and technological

---

[32] Ibid., 21–23.
[33] Ibid., 16.
[34] Ibid., 19–27.

innovations in order to implement a new conceptual approach to warfare or to a specialized sub-branch of warfare.[35] Hundley describes an RMA as a paradigm shift in the nature and conduct of military operations that:

- renders obsolete or irrelevant one or more core competencies of a dominant player;
- creates one or more new competencies in some new dimension of warfare;
- or both.[36]

As in the commercial sector, the initial performance of a disruptive warfighting innovation is such that it underperforms the prevailing warfighting architecture. When initially introduced, this new innovation is typically employed to enhance the performance of the prevailing warfighting architecture. Over time, the performance of the disruptive warfighting innovation improves to the point where it outperforms the prevailing warfighting architecture and emerges as the dominant form of warfare.

The development of naval aviation and carrier warfare illustrate how disruptive innovation can take place in a military context. When first introduced, aircraft had limited range, speed, and payload capabilities. As a result of these limitations, aircraft were first used in the scouting and reconnaissance roles in naval aviation to enhance the performance of battleship warfare. The contribution of aviation to improving the performance of the tactical architecture for battleship warfare is represented in the movement on the solid blue line in figure 4 from point B_2 to B_3. When aircraft were initially introduced, they were launched and recovered from battleships. Over time, as the performance of aircraft improved, aircraft were assigned the mission of securing command of the air over the surface battlespace. Subsequently, as aircraft carrier technology advanced, it became possible for aircraft carriers to launch and recover larger numbers of high performance aircraft that were capable of dropping bombs and launching torpedoes. This innovation is portrayed in the movement from point C_1 to C_2 along the dotted green line in figure 4. Eventually,

---

[35] MacGregor Knox and Williamson Murray, *The Dynamics of Military Revolution, 1300–2050* (Cambridge, UK: Cambridge University Press, 2001), 12.

[36] Hundley, 9–11.

the performance of the combination of aircraft and aircraft carriers increased to the point where carrier task forces had the capability to conduct independent combat operations and carrier warfare could outperform battleship warfare. When point C_3 was reached carrier warfare had effectively "disrupted" battleship warfare as the dominant means of conducting combat between naval forces. Additional examples of sustaining and disruptive warfighting innovations are provided in table 2.
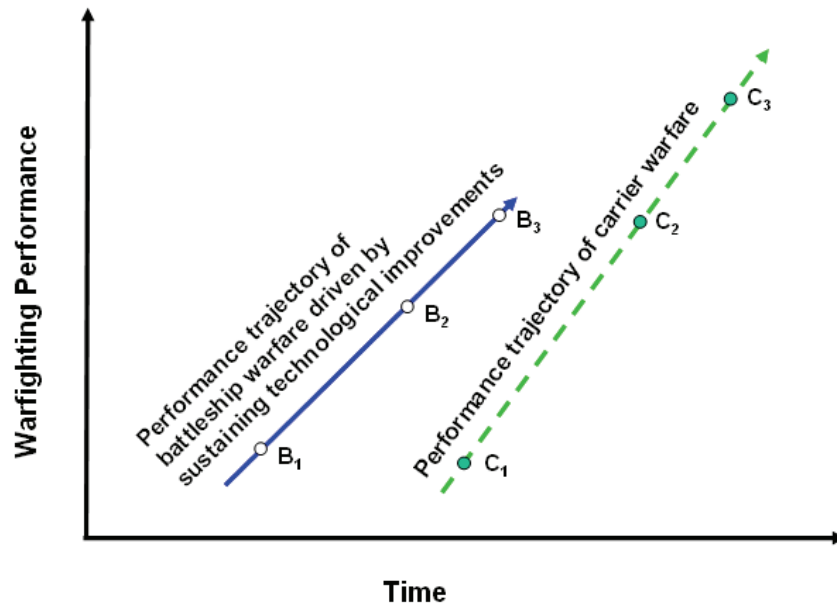
Figure 4: Innovation Trajectories for Battleship and Carrier Warfare[37]

Pierce makes the observation that the application of disruptive innovation theory to historic military innovation helps explain the success and failure of various militaries in pursuing military innovation.[38] In applying the concept of disruptive architectural innovation to military innovation, Pierce highlights the importance of new operational concepts and the importance of examining new

---

[37] This figure is a modification of the figure used in Pierce, 29.
[38] Ibid., 24–32.

Disruptive Architectural Innovations	
USMC Amphibious Warfare	1905–1940
Imperial Japanese Navy Carrier Warfare	1917–1942
USN Carrier Warfare	1918–1943
USN Defensive Sea Control	1970–1974
USMC development of MAGTF Warfare	1975–1989
USN Composite Warfare Commander	1985–1988
USN Maritime Action Groups—Surface Land Attack Warfare	1988–1990
Sustaining Architectural Innovations	
Blitzkrieg	1930–1939
USN Carrier Battle Group	1974–1978
USMC Defensive Advanced Base	1900–1942
USMC MEUSOC Warfare	1976–1988
USMC Prepositioned Logistics	1984–1989
Disruptive Radical Technology Innovations	
USN Aegis Radar	1978–1986
USN Tomahawk Missile	1978–1986
USN Tactical Component Network	1996–2003

Table 2: Examples of Sustaining and Disruptive Innovation.[39]

combinations of technology and doctrine, as well as the important role played by new organizations. Pierce provides evidence that supports his hypothesis that different management methods are required to institutionalize a disruptive innovation. He then describes the critical role played by product champions in managing disruptive innovation. He also highlights the importance of the creation of new career paths in disruptive architectural innovation.[40]

Pierce provides evidence of how "product champions," such as Admiral Moffett and Admiral Yamamoto, initially disguised disruptive innovations as sustaining innovations to reduce organizational resistance and secure resources.[41] He also asserts that the German success in developing blitzkrieg should be categorized as a sustaining

---

[39] Pierce, 18.
[40] Ibid., 32–50.
[41] Ibid., 121–144.

innovation, because it supported the disruptive maneuver warfare and combined arms doctrine developed by General von Seeckt in the early 1920s.[42] In examining the challenges the British and French armies faced in developing armored forces, Pierce identifies the absence of effective product champions as a critical factor in these armies' inability to overcome the challenges of disruptive architectural innovation.[43]

The application of insights from the commercial sector to warfighting innovation provides significant insight into some of the critical factors that influenced historic warfighting innovation. Pierce, in applying the concept of disruptive architectural innovation to warfighting innovation, highlights factors critical to the success or failure of historic warfighting innovation that are absent from the historical record. Combining Pierce's insights with the findings of Leavitt and the MIT90s research provides additional insight into factors that can influence warfighting innovation.

Synthesis of Findings on Innovation

The importance of new operational concepts combined with technology and development of new doctrine and organizations is a theme supported by Murray and Hundley that can be summarized as:

> Unmet military need + new operational concept + new technology + new doctrine + new organizations = new operational capability

Pierce modifies this formula as follows:

> Perceived military need + new operational concept + disruptive technology + new doctrine + new organizations + new career paths + product champions + disguising innovation = new operational capability

Comparing these two themes with the findings of Leavitt provides the motivation for focusing on the elements of technology, process, organization, and people as four primary lines or vectors of innovation. This line of thinking is diagrammed in figure 5.

---

[42] Ibid., 39–50.
[43] Ibid., 32–37.
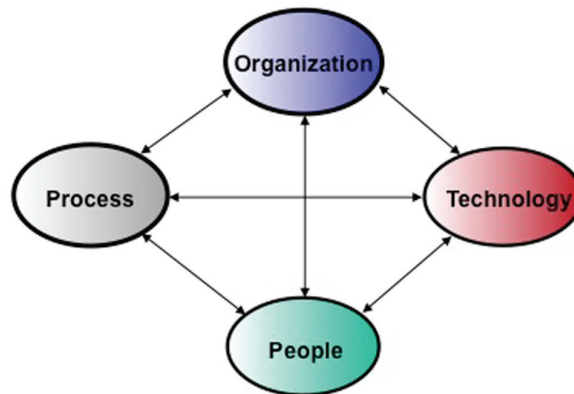
Figure 5: Revised Four-Element Model

Leavitt, in formulating his original diagram, focused on how changes in one element could require changes in one or more of the other elements. These findings are consistent with findings of military innovation. The linkage between technology and doctrine that is involved in architectural innovation described by Pierce is represented by the line between technology and process in figure 5. The creation of viable career paths for naval aviators in the U.S. Navy in the development of carrier warfare is represented by the people element of the model. The creation of the new organizational units of panzer brigades and panzer divisions in the development of blitzkrieg is represented by the organization element. +

The MIT90s research highlighted the relationship between people and organization in creating organizational culture and found that organizational transformation initiatives can be inhibited significantly when proposed changes in the area of people or organization affect organizational culture. As a consequence, the simple four-element model contains the cultural factors that inhibited the ability of the French and British armies to more aggressively pursue the operational implications of armored warfare.

This simple, four-element construct accurately represents the end-state of the architectural innovation described by Pierce and also

highlights factors that can constrain warfighting innovation. The application of the revised four-element model to military innovation provides insights into the challenges of innovation management and a simple model for understanding the role of different types of innovation in capability development.

Comparison with Contemporary Approaches

Applying the simple, four-element model to current military approaches for defining capability yields insights. The U.S. Department of Defense employs a construct referred to as doctrine, organization, training, leadership, material, personnel, and facilities (DOTLMPF).[44] The construct used by the U.K. Ministry of Defence is "defence lines of development," which includes training, equipment, personnel, information, concepts and doctrine, organization, infrastructure, logistics, and interoperability.[45] In the U.K. approach, a concept is defined as "an expression of the capabilities that are likely to be used to accomplish an activity in the future." The Australian Department of Defence construct consists of the following elements: command and management, organization, major systems, personnel, supplies, support, facilities, and collective training.[46] The relationship between these three constructs for describing military capability and the four-element model is portrayed in table 3.

In analyzing table 3, it is clear that there is a close relationship between the four-element model and the elements of the three contemporary military approaches. Facilities and infrastructure seem to be the single major outliers from the four-component model. Combining insights from historic military innovation with contemporary approaches to defining capabilities results in the refined construct portrayed in table 4. This construct identifies processes and key process outputs and also distinguishes between activities that support capability development and activities that directly support the operation of mature capabilities. This construct explicitly addresses concept development, experimentation, and the role of experimental

---

[44] Chairman of the Joint Staffs Manual 3170.01C, Operation of the Joint Capabilities Integration and Development System (1 May 2007), H2-H3.

[45] UK MoD Defence Lines of Development, referenced from the UK MoD Acquisition Operations Framework (V 2.0.18) accessed from http://www.aof.mod.uk/aofcontent/strategic/guide/sg_dlod.htm on 4 Nov 09.

[46] Defence Capability Development Manual 2006 (Canberra, Australia: Defence Publishing Service, 2006), 4-5.

articles. Implicit in the construct is that each process is conducted by an organization that is manned by people with specialized knowledge and skills.

	U.S. Department of Defense	UK Ministry of Defence	Australian Department of Defense
Technology	Material Facilities	Equipment Infrastructure Information Interoperability*	Major systems Facilities Supplies
Process	Doctrine Training	Concepts and doctrine Training Logistics Interoperability*	Collective training Support Command and management
Organization	Organization	Organization	Organization
People	Personnel Leadership and Education	Personnel	Personnel

*Interoperability has both a technology and a process component.

Table 3: Contemporary Approaches for Describing Capability

In analyzing table 4, it is possible to distinguish between the elements of the *capability development processes* and the elements of *operational capability*. The four-element model describes the primary elements of an operational capability as technology, process, organization, and people. This operational capability is developed, supported, and enhanced with a supporting set of processes. These distinct processes are nested and integrated to deliver and sustain operational capabilities.

Processes	Process Output	Relevant Facilities	Process Type
Concept development	Concepts		Development
Experimentation	Insight		Development
Doctrine development	Doctrine Doctrinal interoperability		Development
Personnel	Recruited, promoted, and retained personnel		Development
Education	Educated leaders	Campus/ Labs	Development
Acquisition	Material solutions Experimental articles		Development
Test and evaluation	Tested material solutions	Test Ranges	Development
Interoperability certification	Technical interoperability		Development
Individual training	Individual readiness	Training ranges	Development
Collective training	Unit readiness	Training ranges	Development
Tactics, techniques, and procedures (TTP) development	Tactics		Operations and development
Lessons learned	Insight		Operations
Logistics	Delivered supplies		Operations
Command and management	Effective execution		Operations
Exercises	Readiness		Operations
Operations	Operational readiness	Military bases	Operations

Table 4: Expanded Elements of Capability

Distinguishing between the elements of operational capability and capability development processes yields a valuable insight that can be used to make sense of historic military innovation as well as shed light on capabilities required to manage innovation in the present. The contemporary DOTLMPF construct combines elements of operational capability with a subset of the elements of the capability development process. For example, the doctrine, organization, material, leadership and personnel correspond to process, organization, technology, and

people (which combines personnel and leadership). Operational forces are composed of these elements of capability. Training is the process used to prepare forces for operations. The output of the training process is forces with increased operational readiness. Material solutions are an output of the acquisition process. New operational concepts are the output of the concept development process. Similarly, the output of experimentation is insight in the potential effectiveness of new operational concepts. The key point here is that the processes that a military organization must use to develop new concepts and translate them to operational capabilities are not defined by the DOTLMPF construct.

Developing new concepts and translating them to operational capabilities requires organizations to be able to innovate in a range of areas and on different timescales. The innovation involved in the development of new tactical architectures involves innovation on a large scale, involves multiple lines of development, and can play out over years to tens of years. The technology innovation involved in developing a new material solution may play out over years to tens of years. The process innovation involved in the development of new tactics, techniques, and procedures can play out on much shorter timescales. Similarly, the innovation involved in developing a personnel system may play out over a period of a few years. One of the major challenges of military innovation lies in linking and synchronizing innovation in two or more lines of development.

Creating the Capability to Manage Innovation

All historic architectural innovation has required the management of innovation in a number of lines of development. One of the critical factors in the success of historic architectural innovation has been the ability of an organization to develop the capability for managing and integrating innovation across multiple lines of development.

One of the best examples of the importance of developing a capability for managing innovation is provided by the development of carrier warfare by the U.S. Navy. Admiral (then Captain) Moffett realized that to effectively manage and oversee the disparate activities related to aviation that were being conducted within the U.S Navy, a new organization needed to be created with powers equivalent to the existing Bureau of Navigation. He testified before the House and Senate naval affairs committees regarding the benefits of creating a stand-alone bureau focused on aviation. President Harding

subsequently signed a bill into law that authorized the creation of the Bureau of Aeronautics on July 13, 1921, and a week later nominated Moffett as the bureau's first chief.[47] This organizational innovation was a critical step in the development of carrier aviation. Once this organization had been established, Moffett proceeded to develop the capability for managing all aspects of naval aviation. The Bureau of Aeronautics had responsibility for overseeing the development of material solutions and experimental articles (technology innovation), training aviators (process and infrastructure innovation), developing new TTPs[48] (process innovation), establishing a viable career path for naval aviators (people innovation), and assessing the military utility of carrier aviation through experimentation and wargaming (process innovation).

The Bureau of Aeronautics, an organizational innovation, had to be created before the broader innovation process associated with aviation could be effectively managed. In other words, creating the capability for effectively managing the innovation associated with aviation and carrier warfare was a critical success factor in the overall innovation process. Over time, the Bureau of Aeronautics acquired the resources, developed the processes, and established organizational values that were critical to the development of carrier warfare.

This observation leads one to think about military innovation in terms of both the capability for managing innovation and the capability for conducting innovation in the areas of concepts, technology, process, organization, and people. A simple model of the innovation management process and synchronizing innovation in these five areas is portrayed in figure 6.

---

[47] Pierce, 124.
[48] Tactics, techniques, and procedures.
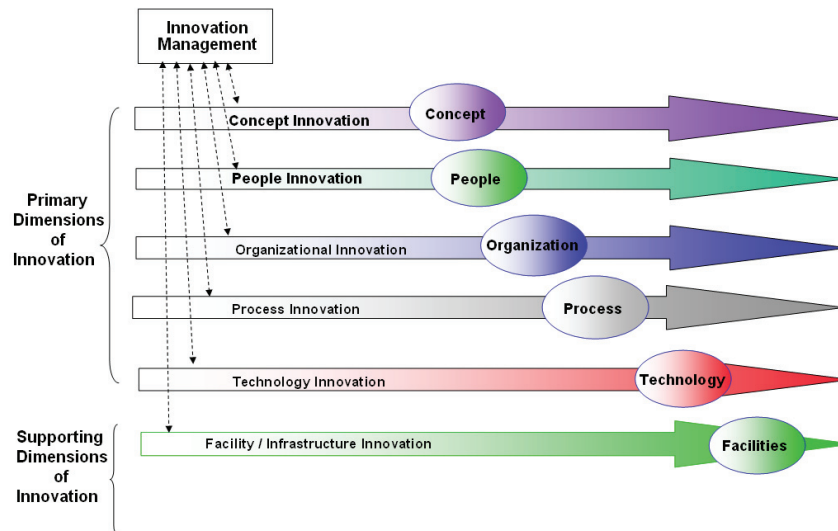
Figure 6: Model of Innovation Management

Representing Architectural Innovation

The evolution of a tactical architecture over time can be portrayed graphically, as shown in figures 7 though 10. These diagrams depict the relationships between the four lines of innovation and the evolving state of a tactical architecture. An initial tactical architecture is represented in figure 7. Figure 8 depicts a future state of this tactical architecture that corresponds to a situation in which technology has advanced, but doctrine or TTPs are lagging. The situation that exists where process innovation has caught up with technology innovation is portrayed in figure 9. A situation also can exist where several iterations of technology–process innovation take place before organizational or people innovation advance further. Figure 10 portrays the state of a tactical architecture in which organizational innovation and people innovation have advanced and a tactical architecture has reached an initial operational capability.

Figure 7: Initial Tactical Architecture

Figure 8: Technology Innovation Leading

Figure 9: Linking Process Innovation with Technology Innovation
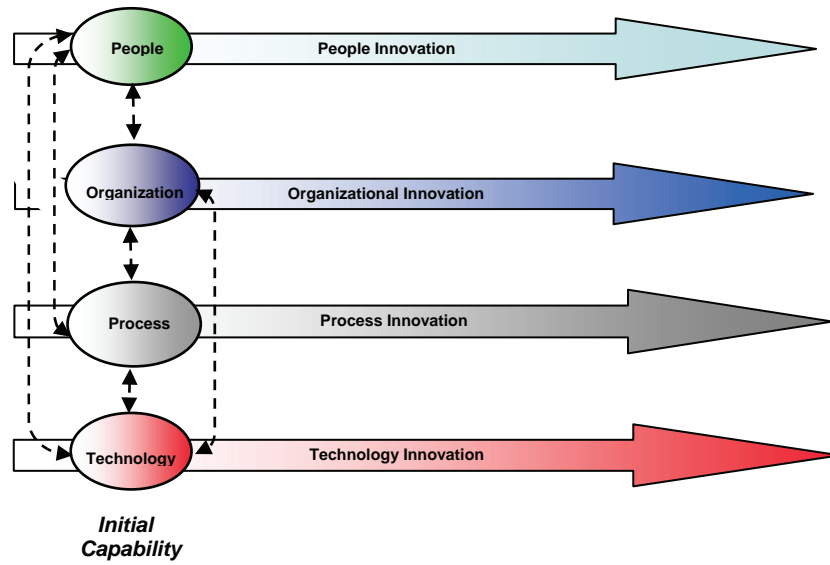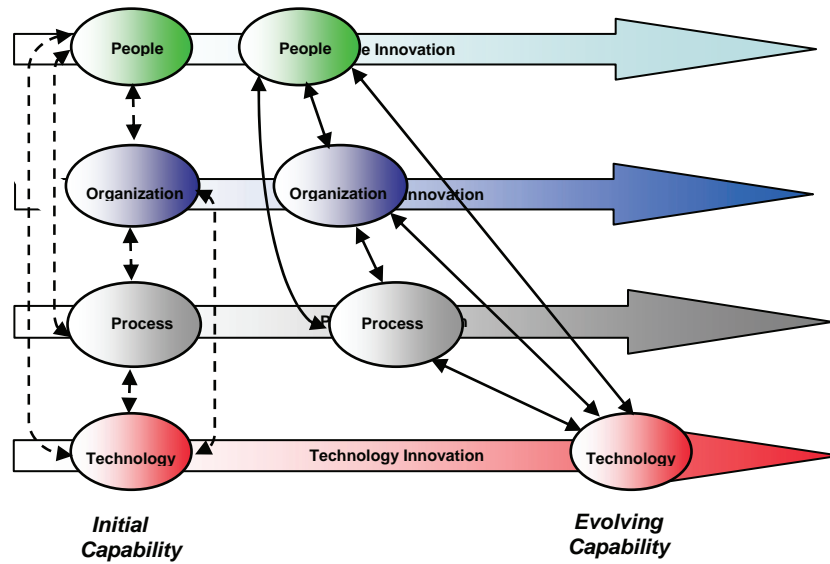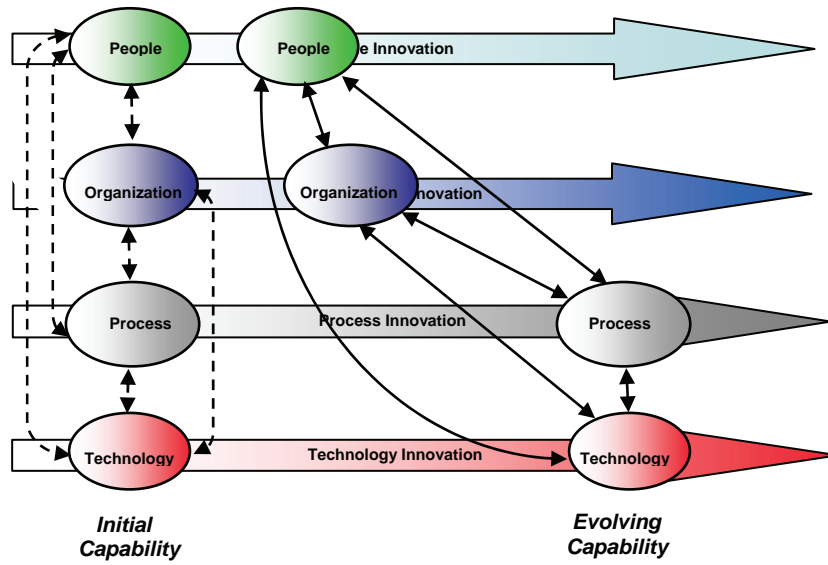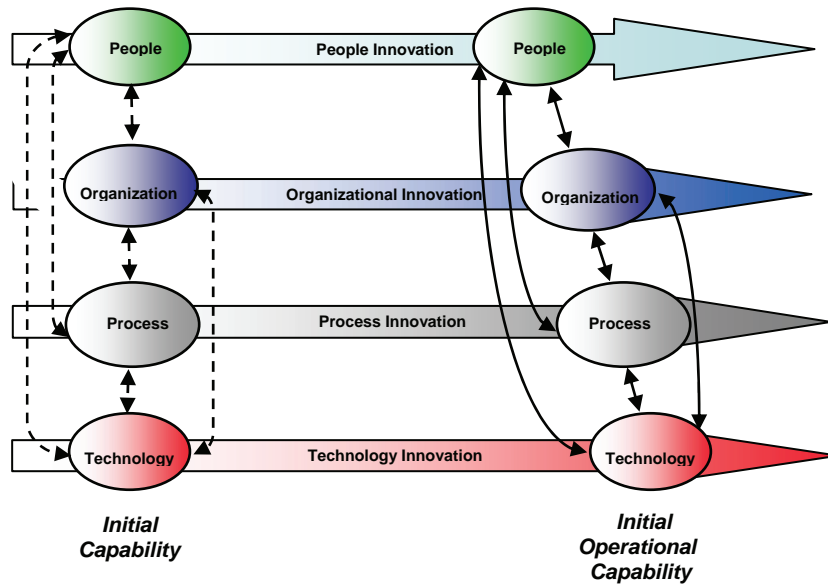

Figure 10: Tactical Architecture at Initial Operational Capability

The pattern of successive iterative innovation in the four primary lines of development, combined with refinements to theory and operational concepts and the application of disguising innovation, occurred in the successful development of a range of tactical architectures. The relative magnitude and importance of the technology, process, organization, and people innovations varied in each case of disruptive tactical architecture innovation. However, the underlying pattern of connected innovation is constant across all cases.

The development of amphibious warfare and carrier warfare provide examples of connected innovation. The order in which major innovations occurred in the development of amphibious warfare is presented in table 5. This order is noteworthy, in that the development of mature technology significantly lagged the development of doctrine and organization. The timing and sequencing of the innovation involved in the U.S. Navy development of aviation, carrier aviation, and carrier warfare is presented chronologically in table 6. This table captures selected highlights of a period of extensive innovation that took place over a period of 32 years and included the extensive use of Naval Aviation during World War I and World War II.

Date	Dimension of Innovation	Area	Example
1921	Theory/concept development	Strategy	Advance base operations in Micronesia
1921	Process	Plans	Plan 712D–part of Plan Orange
1933	Organization	Organization	Fleet Marine Force
1933	Organization	Innovation organization for technology	The Marine Corps Equipment Board was the first U.S. professional body focused on the development of material suitable for use by forces conducting amphibious warfare.
1934	Organization	Innovation organization for doctrine	Marine Corps School at Quantico—school shut down for 6 months in 1934 to develop doctrine for amphibious warfare
1935	Process	Doctrine	Tentative Manual for Landing Operations
1941	Technology	Advanced technology for amphibious warfare	Higgins Boat—Landing Craft Vehicle, Personnel (LCVP) Landing Ship Tank (LST)
1934–1941	Process	Exercises	Fleet landing exercises
1934–1941	Technology	Early technology for amphibious warfare	Dock loading equipment

Table 5: Timeline of Key Events in the Development of Amphibious Warfare[49]

---

[49] Ibid., 51–69.

Date	Dimension of Innovation	Area	Example
1908	Organization	Organization	Creation of general board
1909	Theory/concept development	Early concept	First reports on viability of naval aviation filed
1911	Technology	Material	First funds appropriated for "Experimental work in the development of aviation for Naval purposes"
1911	People	Personnel	First naval aviator qualified.
1911–1914	Technology	Material	Aircraft Development
1914	Facilities	Facilities	Establishment of Naval Aeronautic Station Pensacola—pilot training base
1914	Process	Training	Initiation and standardization of pilot training
1914	Process	Education	Establishment of aeronautical engineering program at MIT
1916	Technology	Material	First experiments with radio
1916	Organization	Organization	Establishment of Naval Flying Corps
1917	Technology	Material	Initiation of prototype aircraft production
1920	People	Personnel	"Authority to draw best graduates of the U.S. Naval Academy into aviation"
1921	Organization	Organization	Establishment of Bureau of Aeronautics
1921	People	Leadership	Moffett named first Chief of Bureau of Aeronautics; serves for 12 years until his death in an accident in 1933
1922	Technology	Experimental article	Experimental carrier Langley (CV-1)
1923	Process	War games	Naval War College initiates tactical war games focused on carrier aviation and carrier warfare.
1923	Process	Exercises	Initiation of fleet problems—aviation used in Fleet Problem I.
1925	People	Leadership	Reeves selected as commander, Aircraft Squadron, Battle Fleet, with USS Langley as his flagship
1925-1926	People	Personnel	Policy created by which only aviators could be selected to command aircraft carriers and stations.
1927	Process	Doctrine/ TTP	Development of TTP for launch, recovery, and attack
1927	Process	Doctrine	Importance of "knock-out" blow against enemy air power in the opening minutes of a confrontation.
1927	Organization	Organization	Establishment of small innovation group to "explore all aspects of aviation"
1927–1941	Technology	Material	Carrier development (CV-2 through CV-8)
1931	Theory/concept development	Theory	New theory of warfare for carrier aviation described by Moffett in memo to the secretary of the Navy
1931	Organization	Organization	Establishment of small innovation group to develop fleet carrier doctrine
1933	Process	Doctrine	Development of PAC-10—basic carrier doctrine for the Pacific
1942	People	Personnel	Creation of the aviation-type commander
1942	People	Leadership	Admiral King is first aviator selected to be Chief of Naval Operations.

Table 6. Timeline of Key Events in Development of Aviation and Carrier Warfare[50][51]

---

[50] Pierce, 121–131.

[51] The History of Naval Aviation, *A Few Pioneers: 1898–1916; Test of Strength: 1917–1919; The Twenties: 1920–1929; The Thirties; World War II;* accessed at http://www.historycentral.com/Navy/chron/

Innovation Management for Tactical Architectural Innovation

In the commercial sector, disruptive innovation creates problems because challenged organizations have business models, values, and organizational cultures that impede an effective organizational response. Organizational values and culture can similarly impede a military organization's ability to pursue certain types of innovation. Pierce found that one of the most important roles played by product champions was disarming these organizational defense mechanisms.[52]

In the development of armored warfare, both the British and French armies were constrained to a large degree by organizational values, attitudes, and cultures that precluded them from effectively moving past the primary role of tanks as infantry support weapons.

In the French army, the prevailing attitude was that neither 1-year conscripts nor reservists could be effectively trained to conduct offensive military operations.[53] In the early 1930s, Colonel Charles DeGaulle lobbied for the adoption of a professional army. His concept was to create seven divisions comprising 100,000 soldiers serving a 6-year tour of duty. In his mind, it was clear that only highly trained professional soldiers were capable of conducting offensive military operations. Creating a large standing army was viewed by the Left as a threat to the Republic and was politically unacceptable. The social political environment of the 1930s resulted in the French army closing ranks, shutting down internal debate, and focusing on internal preservation.[54]

In the British army, the prevailing attitudes of the cavalry toward the importance of the morale element of war and the cavalry's focus on tradition impeded a broader examination of the potential role of armored warfare.[55] As Pierce observes, the British army lacked an effective product champion capable of disguising the disruptive nature of armored warfare.[56] The efforts of advocates for armored warfare, Liddell Hart and Fuller, were overly disruptive and placed the broader organization into a defensive mindset. Even when faced with evidence of successful experimentation that explored the operational utility of

---

NAVALAVIATION.html on 14 May 2009.
[52] Pierce, 192–201.
[53] Keir, 73–83.
[54] Ibid., 85–86.
[55] Kier, 136–137.
[56] Pierce, 32–37.

armored forces, senior British Army officers were unable to make changes that they felt would affect the culture they valued so highly.[57]

The pattern of innovation in both the British and French armies is portrayed in figure 8. Both armies supported technology innovation and developed tactics for using tanks as infantry support weapons. Both armies trained personnel to operate tanks in this capacity. However, in both cases, constraints relating to people, organization, and culture impeded further innovation in armored warfare.

Historically, the success or failure of tactical architecture innovations has been dependent on the success of a product champion successfully positioning an innovation in a manner that enabled existing organizational leadership to support it. Pierce found that this positioning was accomplished by disguising the initial phases of a disruptive tactical architectural innovation as a sustaining innovation that enhanced the warfighting capability of the prevailing tactical architecture.[58] This disguising is primarily required to address the challenges of intraservice competition.

In the development of carrier warfare both by the U.S. Navy and the Imperial Japanese Navy, product champions disguised the initial phases of the development of carrier warfare as sustaining innovations. This disguising involved focusing on the role of aviation in conducting reconnaissance, spotting, and securing command of the air over the surface battle space, as opposed to using independent air operations to attack an enemy fleet.[59] In both cases, interservice competition with the advocates for land-based aviation enhanced the support for aviation within the navies.

The importance of the disguising approach can be understood by examining figure 4 and figures 8 through 10. The increase in performance of the tactical architecture for battleship warfare over time is portrayed with the movement from point B_1 to point B_3 on the solid blue line. Performance improvements realized in moving from point B_2 to point B_3 correspond to the improvements enabled by the employment of aircraft as spotters and scouts, which improved the realizable range and accuracy that could be achieved by a battleship's main guns.

---

[57] Ibid.

[58] Ibid., 196–197.

[59] Ibid., 127–130, 135–140.

The trajectory of innovation for carrier warfare is portrayed by the dotted green line in figure 4. The innovation involved in the development of the tactical architecture for carrier warfare is portrayed in figures 8 through 10. Figure 8 corresponds to a phase in the innovation process in which technology innovation leads other types of innovation. This could correspond to the situation in which carriers could launch and recover aircraft, and the primary mission of carrier aviation was being debated. Figure 9 corresponds to a point at which process innovation has occurred and is now synchronized with technology innovation. This phase of development, when carriers could conduct offensive operations to attack enemy fleets, corresponds to point C_2. At this point, both Yamamoto and Moffett communicated to the proponents of battleship warfare the sustaining role of carrier aviation in supporting the main battle, which would be conducted by battleships. This obfuscation was necessary to maintain funding for carrier aviation until more mature tactical architectures for carrier warfare had been fully developed. The full development of these tactical architectures corresponded to the capability to conduct multi-carrier operations, represented by point C_3 in figure 4.

Implications for Capability Development

Yamamoto and Moffett both realized that their respective organizations would be taking on unacceptable levels of future operational risk if they did not pursue the development of carrier aviation and carrier warfare. The key to their success was recognition that the disruptive nature of carrier warfare required a disguising approach to manage internal organizational risk.

Architectural innovations are the exception rather than the norm. Leaders in most military organizations can spend an entire career and never be faced with the challenges of disruptive architectural innovation or of creating a new competency in a new dimension of warfare. They are far more likely to be faced with the responsibility of leading or managing innovations in one to two areas, or to be faced with the challenge of leading sustaining innovation.

Regardless of the type of innovation being pursued (sustaining or disruptive), the technology, process, organization, and people model provides a useful framework for understanding the role of different types of innovation in capability development. The model provides a simple framework for classifying lines of development and visualizing the evolution of tactical architectures.

From a practitioner's perspective, the primary and supporting lines of innovation approach highlights the principal types of innovation that need to be considered in developing new capabilities or enhancing existing capabilities. Leaders can benefit from knowledge of the relationships highlighted in this model when faced with the challenge of leading or contributing to the successful implementation of large-scale organizational change or capability development initiatives. By focusing on the relationships between the lines of innovation, as well as the timing and sequencing of the lines of innovation, leaders will increase their probability of success in developing or enhancing capabilities.

Disruptive innovation poses challenges to both military and commercial organizations. Christensen and Pierce both highlight the key role that leaders must play in successfully championing a disruptive innovation and overcoming impediments created by prevailing organizational values and culture. Leaders who are unaware of the differences between sustaining and disruptive innovation are unlikely to succeed when faced with the challenges posed by disruptive innovation. Based on the historical record, disruptive warfighting innovations have the potential to be high-impact events. Consequently, military leaders need to be aware of this type of innovation to be able to successfully respond to the moves of potential adversaries or to successfully lead a disruptive innovation. As Christensen and Overdorf found, leaders, when faced with the challenge of disruptive innovation, must often create new organizations with processes and values required to respond to a competitor's actions. These actions can be particularly challenging in a military environment.

Summary and Conclusions

Organizations need to have the capability to innovate to respond effectively to challenges and opportunities. Consequently, innovation is an organizational capability that is important in commercial, government, and military organizations. Different types of innovation can pose distinct challenges to organizations. Insights from the commercial sector and historic military innovation can help leaders develop an understanding of the nuances of innovation. Key aspects of innovation discussed in this essay are summarized below.

- Innovation can occur in the lines of development of people, process, organization, and technology.

- There are four types of technology innovation: incremental, modular, architectural, and radical.
- Innovations in one line of development often require innovations or changes in other lines of development.
- Architectural innovation can take place at two levels: the system level and the tactical architecture level.
- Innovations can be either sustaining or disruptive.
- An organization's capabilities for innovating are both enabled and constrained by resources, processes, and values.
- Disruptive tactical architectural innovations are at the core of revolutions in military affairs.
- Disruptive innovations may need to be managed by disguising them as sustaining innovations to reduce organizational resistance and secure resources.
- Managing disruptive innovations as though they were sustaining innovations invariably results in failure.
- Military innovation can be amplified or attenuated by macrofactors such as interservice and intraservice rivalry.
- Organizational culture is a key determinant in an organization's ability to innovate.

The need for military organizations to be able to innovate in the areas of technology, process, organization, and people will persist as long as military organizations exist. With this backdrop, the innovation concepts discussed in this essay provide a framework for understanding the past, interpreting the present, and preparing for the future.

Essay 3

Delivering Network-Enabled Capability

The Importance of Innovation in Delivering Culture Change

By Derrick Neal and Louise Carver

Abstract

Research reported by Neal & Taylor (2006) has highlighted the challenges faced to bring about change within the MoD, and it is argued that too much emphasis has been placed on the levers of organisational structures and systems/processes to drive change forward and too little on the people dimension. This paper argues that, to achieve the full benefits of Network Enabled Capability (NEC), the MoD needs to give serious consideration to how it can develop an NEC culture through a change program that gives due care and attention to modifying a number of elements, such as attitudes, reward systems, symbols, and behaviours that contribute to shaping the culture of the organisation. The starting point for any change programme is the establishment of the nature of the problem and the recognition that the problem needs to be communicated to those involved. The usual military approach is to conduct a training needs analysis (TNA) that is intended to identify the gap between where we are now and where we wish to be in the future. In the case of NEC, research already conducted has suggested that key players have not embraced the concept with the enthusiasm that may have been anticipated, and the view currently held is that the MoD does not yet have an NEC culture. Furthermore, it is apparent that the requisite support structures are not yet in place or fully exploited to ensure that all MoD personnel are aware of and can access training, education, and information to develop further their abilities to operate in a networked information environment.

The paper presents preliminary findings from semi-structured interviews and analysis of primary data and provides insights as to the nature of the challenge that is faced by the MoD.

Introduction

Network-enabled capability (NEC) is not a new concept. The power of networks was clear to the Romans, who used an extensive network of roads to run a huge empire. The outcome of the Battle of Britain was arguably determined by exploiting networked information. Rapid technological advances have provided us with the means to acquire information from a variety of sources and make it available to decision-makers to achieve military effect. However, it is clear that it is the human factor—the skills, knowledge, experience, and attributes of those involved in managing and exploiting that information—that makes NEC powerful.

The U.S. Armed Forces and Australian Defence Force (ADF) have made significant advances in their development of network-centric operations (NCO) and network-centric warfare (NCW), respectively, and we should capitalize on the lessons these organizations have already identified. In Operation *Iraqi Freedom*, the U.S. Armed Forces "clearly demonstrated their asymmetric advantage . . . in such high intensity interstate warfighting" through "dramatically increased situational awareness."[1] The paper further states that, "the key was their information and their ability to act on it within the available window of opportunity." Within the ADF, the NCW capability requirement is defined as "the integration of the information network with a series of grids (Command and Control, Sensor and Engagement) that facilitate cooperative activity by Defence personnel."[2] The ADF experience of operations with coalition partners in Iraq and Afghanistan has demonstrated "the potential operational benefits of NCW." There is also recognition within the ADF of the potential for "unforeseen innovation" and of the opportunity to "maximise the potential for development of an NCW capability via the partnerships that will result from initiatives." A study addressing the human dimension of NCW recommended that NCW awareness be raised through brochures and a road show, that senior leaders be appropriately educated about NCW concepts, that future leaders in the NCW era be prepared, that future workforce requirements be reviewed, that NCW tools be developed,

---

[1] *Future Conflict: Insights from Interviews with Senior Commanders.* January 2006.

[2] Australian Government Department of Defence, *NCW Roadmap*, 2007.

and that a mechanism for evaluating and feeding back lessons learned into future collective training activities be developed.

The NEC Handbook

The U.K. position is slightly different in some aspects. Although NEC shares the tenets of NCO, it is more limited in scope, in that at the time Joint Service Publication 777 (JSP 777), the NEC handbook, was written, it was not seen as a doctrine or vision.[3] However, since then, it is probably fair to say that NEC has evolved into a vision that is currently being pursued. NEC does not seek to place the network at the center of capability in the doctrinal way that NCO implies. Rather, NEC is much more concerned with evolving capability by bringing together decision-makers, sensors, and weapon systems and enabling them to pool their information by networking to achieve an enhanced capability.

The production of JSP 777 was intended to raise awareness of NEC, develop a common understanding within the wider defense community, and situate the concept within the perspective of where the Ministry of Defense (MoD) is heading. In this regard, the Joint High Level Operating Concept (Jt HLOC) was endorsed by the Chiefs of Staff in 2004 as the head-mark for how we should seek to conduct military operations in 2020. NEC is at the heart of the way of operating described in Jt HLOC. However, since Jt HLOC was written, the U.K. Armed Forces have gained considerable experience in Afghanistan and Iraq and have seen suicide bombers blowing up targets in London. Therefore, we need to assess continually how the evolving nature of the conflicts in which we become involved affect our command and inform and operate capabilities and to draw key deductions that should shape the development of those capabilities.

NEC should be viewed as an enabler of mission command (one of the key underlying principles of the U.K. military), giving it new expression by allowing it to thrive in a context in which the commander can articulate his intent and then allow subordinate commanders to execute that intent in the knowledge that they share the same situational understanding, thus negating the need to interfere unless absolutely necessary. JSP 777 highlights four dimensions of NEC—networks, information, people, and joint action (see figure 1)—which overlap and

---

[3] Joint Service Publication 777, *Network Enabled Capability*, edition 1 (London: Ministry of Defense, 2005).

are mutually dependent. All of these dimensions need to be developed and managed for NEC to be fully realized. The dimensions of and challenges associated with the delivery of NEC within the U.K. MoD were highlighted and discussed in a paper by Neal (2007) that explored the issues of delivering NEC by drawing on classical change management theory and postulating how the gaps in the MoD's application of NEC need to be addressed.
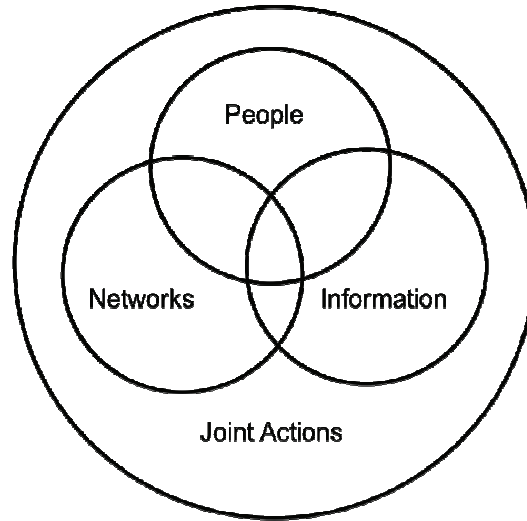
Figure 1: The Four Interdependent Elements of NEC

Matters have not been helped by the fact that since the late 1990s, the U.K. military has been under significant pressure from operational commitments, which have ramped up significantly since 2003. One consequence of this level of military activity is that the MoD finds itself having to deal with urgent operational requirements (UORs) and urgent operational tasks (UOTs). As a consequence, significant resources have had to be diverted to direct support to operations. The solutions to UORs and UOTs are delivered into theater, quite rightly, for a particular purpose, but this may also be at the expense of the necessary coherence of the larger equipment program intended to deliver NEC structures and systems and the development of a truly joined-up acquisition process that is part of an MoD-wide enterprise architecture. Indeed, some involved in the UOR/UOT process are quite clear that capability delivered through it is unlikely to fit with longer-term plans but that, until the requirements, planning, and resourcing

mechanisms are sufficiently coherent, flexible, and responsive to address changing and unforeseen needs, users will continue to rely on the process to meet immediate operational needs

It might be argued that, had the MoD put in place the doctrinal approach at the outset, some of these issues may have been more readily identifiable; however, it was never the intention in the United Kingdom to take such an approach from the outset. Indeed, it is noted very clearly in JSP 777 that the approach to change would be based on evolution, and as such, three stages had been clearly identified:

Initial. Based on *current doctrine*, organizations, processes, and equipment where improvements to operational capability can be made in the short term. It is characterized by minor organizational changes and equipment enhancements, such as using data links to replace voice. Work to achieve this state will be characterized by *interconnection*.

Transitional. Medium-term improvements in operational capability will be generated by *incremental changes to current doctrine*, processes, training, and equipment, validated by appropriate experimentation and exercises as part of the development cycle. This will be supported by major organizational change and the integration of technical systems to give greatly improved shared situational awareness (SSA) through better information management. Work to achieve this state will be characterized by *integration*.

Mature. Maximum advantage will be gained from the optimal exploitation of information, delivered through *developed doctrine,* organizations, processes, and equipment, together with personnel appropriately selected, educated, and trained. It is typified by the dynamic creation of mission groups enabled by distributed collaborative working. This longer-term evolution is built on the lessons learned from the earlier states. Work to achieve this state will be characterized by *synchronization*.

Why Are the People Issues So Difficult to Resolve?

There are a number of reasons why the people dimension provides a major challenge in terms of delivering effective NEC, and they relate back directly to the literature on change management, in that humans are generally resistant to change. This is particularly true in situations in which there is no perceived "burning platform" that compels individuals or organizations to change. What might such a burning platform look like? At one extreme it might be the United Kingdom

finding itself in a conventional war with a nation that has a superior observe, orient, decide, and act (OODA) loop and is inflicting significant losses on U.K. military forces. Another might relate to the government of the day facing sufficient public pressure to spend taxpayers' money on public services other than defense. There might also be the risk that the United Kingdom's inability to keep pace with major allies in improving the delivery of military effect would result in its being consigned a far less influential role on the world stage.

However, the reality is that we are fighting new types of foes who are prepared to wage a long war and operate in ways that have not formed a major part of our education and training processes to date. The changing nature of threat has long been understood by military machines and expressed in the concern that, "if you prepare for future wars based on how you fought the last war, you will fail." Management has its parallels, as expressed by Hamel & Prahalad (1996) in the notion that underpinning strategies 1 and 2, as shown in figure 2, are about catching up with your competitors and will always leave you at risk. It is the paradigm shift in option 3 that will put you in a position to drive the agenda. It might be argued that the current military operations in Afghanistan and Iraq are having to adapt to an enemy that has rewritten many of the rules of engagement and is defining the nature of the conflict, and to a certain extent Western forces are continually having to adapt and morph their responses. Perhaps this is overly harsh because, within the spectrum of NEC activity, there are clear examples where NEC technology has saved lives and continues to do so. One case in point is that of Blue Force Tracker, which has helped to reduce the incidence of friendly fire incidents. Another is the success that has been achieved with the application of OVERTASK in Afghanistan, where integrated decision loops have significantly reduced critical timescales in a number of aspects of the military machine and have promoted more joint operational applications, such as JADOCS and JChat, which in themselves promote a different set of behaviors that are consistent with the NEC philosophy.

A particular challenge for the MoD in getting commitment to change is that most military staff are only in post for a maximum of 3 years; indeed, given the current level of operations, many are unlikely to stay in the same post for more than 18 months. This high level of churn, as reported by Neal & Taylor (2006), can be a major barrier to real change being delivered within an organization. Comparatively

speaking, the civilian community is somewhat more stable (although this is changing, and civil servants are becoming more mobile), and so,
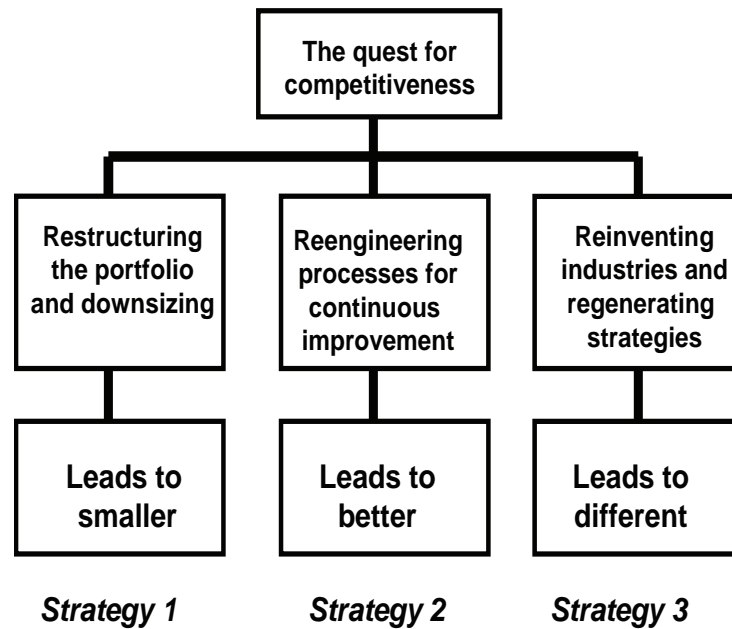
```
                    ┌─────────────────┐
                    │  The quest for  │
                    │ competitiveness │
                    └─────────────────┘
```

Restructuring the portfolio and downsizing	Reengineering processes for continuous improvement	Reinventing industries and regenerating strategies
Leads to smaller	**Leads to better**	**Leads to different**
Strategy 1	*Strategy 2*	*Strategy 3*

Figure 2: Generic Strategic Options (Source: Hamel and Prahalad, 1996)

in effect, there are those who may be in a post for several years who can "sit out" the changes initiated by military staff, or appear to support the change but actually deliver very little. This situation is well known in the change management literature, where such people are referred to as "worried stayers." When talking to staff in organizations in which this dynamic exists, it is common to hear people talking about "change fatigue" and a lack of commitment, and the fact that no change is ever in place long enough to see the benefits because they have already moved to the next iteration. Furthermore, there is a tendency to see change as being driven and imposed from elsewhere, with little or no attempt to summarize the progress made before change was required or to explain why more change is required. Therefore, change initiatives are viewed, not surprisingly, with a considerable degree of weary cynicism. Specifically, within the NEC change perspective it is also important to recognize that there is a symbiotic relationship between equipment (and systems/processes/software) and humans, such that the operator will exhibit behavior that reflects the equipment, and the

equipment design will have been considered in terms of how humans behave. As a consequence, it can be a real challenge to break an existing paradigm, as it needs to reflect both facets simultaneously. Within the business environment, there are reported cases of senior management having to force the issue of the need for change by breaking the current systems and structures that act as a straitjacket on the behaviors of staff. Such an approach is not feasible within the domain of the military, as it can result in military personnel losing their lives through major systems failures.

By definition, NEC is a facilitator of dispersed teams working in real time (or near real time), with decision-making having to take place in an increasingly information-rich environment. The work of Looy-Hyde (2007) is particularly helpful in this regard, as she highlights the findings from industry and academia in terms of the factors and issues that need to be resolved for dispersed team working to be successful.

For example, within the military, the notion of SSA and joint common operational picture (JCOP) are well understood, and we spend a great deal of time and effort to put in place technology/systems and training (individual and collective) to deliver SSA. Sonnenwald et al. (2004) defined SSA as "knowing about things that are happening in the immediate environment, [the environment of others] … and having an accurate understanding of the situation and the knowledge to respond appropriately as the situation evolves."

However, there is a significant difference between SSA and shared situational understanding (SSU), and the real risk is that one assumes that understanding is achieved. Bechky (1999) highlighted the fact that knowledge being exchanged through a computer-mediated environment, as opposed to face to face, can cause problems for team members from different roles as they struggle to understand one another.

Looy-Hyde (2007) also draws attention to some of the consequential problems that flow from dispersed teams, as noted by Cramton (2001), who identified five key issues:

- failure to communicate and retain contextual information,
- an uneven distribution of information,
- differences in salience of information,
- speed of access to information, and
- the interpretation of the meaning of silence (nonresponse).

As noted by Looy-Hyde (2007), the accurate interpretation and retention of information are problems that may still challenge the military, despite significant investment in state-of-the-art situational awareness (SA) communications tools. Although it is technically feasible to share information, one still must confront the issue of the "illusion of shared understanding," as noted by Gibson & Cohen (2003), which can be exacerbated by cultural differences. There are, of course, a number of dimensions to this issue, and although a military may train in a joint environment and operate with a joint capability, there remains an element of single-service culture that can result in misunderstandings. Increasingly, in a NEC environment, the pool of information is being used by civil servants within the MoD in support to operations, other coalition partners, other government departments (OGDs), and nongovernmental organizations (NGOs) and, therefore, both organizational and national cultures have a potential for disrupting a SSU.

One of the most significant barriers to achieving SSU is related to the difficulty of communicating social information, such as preferred communication style (hence the difficulty in developing a rapport), as this is often neglected in favor of task-related information, according to Chidaranbaram (1996). Such lack of focus is particularly damaging, as it results in communication becoming transaction-based, rather than relationship-based. Within a hastily formed network scenario, insufficient effort is devoted to developing a mutual understanding of ways of working and information priorities. To some extent, this results in individuals positioning themselves from the perspective of delivering the basic minimum service (from their view), which can very quickly lead to misunderstandings. It also means that, for any individual in a network, there will exist relationships that cover a spectrum of shared understanding and basis for working together. In some cases, parts of the network will work together frequently and over a period of time (and perhaps even hold the occasional meeting face-to-face), such that a degree of social exchange will take place and mutual understanding and trust will be developed. However, at the other end of the spectrum, no time or effort is devoted to this, parts of the network are simply users or suppliers of information, and there is little scope for mutual trust and understanding to be developed—which works against the aspirations of the NEC concept.

Looy-Hyde (2007) and other researchers, such as Warkentin et al. (1997), Walther & Burgoon (1992), and Jones & George (1998),

highlight the importance of interpersonal relationships and, in particular, the importance of mutual trust, and they present findings from a number of studies that confirm that trust plays an important role in successful dispersed teamworking. The material presented by Looy-Hyde (2007) suggests that ad hoc teams may benefit from developing relationships quickly. However, this aspiration is hindered by the lack of face-to-face communication. She explains the concept of swift trust by noting the following:

> There is research to suggest that trust is not always a necessity for effective task completion (Jarvenpaa & Leidner (1999)) and virtual team members are able to accomplish tasks without developing deep relationships but by developing "swift trust." Out of twelve newly formed teams, those that were most able to cope with technological and task uncertainty and to resolve conflicts and problems were teams that formed trust quickly or "swift trust" (Meyerson et al (1996)). Unlike traditional trust, which develops over time as a result of shared experiences, interactions and social norms (e.g. Meyerson et al (1996)), *"swift trust" develops amongst groups that initially exchange social information, enthusiasm, make others aware of their own constraints and show initiative* (Jarvenpaa & Leidner (1999)). In times when teams are quickly formed and quickly disbanded, as is likely to be the case with a task based approach, the development of swift trust may be critical." (emphasis added; Looy-Hyde, 2007, 5)

The activities and assets required to realize effects within a comprehensive approach will necessitate a greater degree of interaction with OGDs, NGOs, and allies, and if interaction between these elements is to be optimized, there is a requirement not only for the technical infrastructure to support collaborative working, but also for the development of common understanding across all elements regarding how they can work together effectively and the norms of behavior that govern these interactions.

The People Dimension Steering Group and the Basis for the Current Research.

The People Dimension Steering Group (PDSG) is responsible for the People Line of Development of NEC and aims to generate capable and motivated personnel who, individually and collectively, can exploit the benefits and mitigate the risks of NEC. To achieve this, the PDSG has commissioned a number of strands of research work to help understand more fully the range of issues that need to be addressed and

shed light on the interactions between each of the strands of activity. The piece of research presented in this essay is intended to help inform the training and education interventions needed to deliver motivated, capable people for the NEC sociotechnical system and grow the accompanying culture and behaviors.

The Research Methodology

The project team examined sources of evidence from within the operational and business space and analyzed these sources to draw out key themes. These themes were then categorized into components and behaviors that may help or hinder the effective delivery of NEC. The findings were put to representatives from across the MoD by way of semistructured interviews to test their validity and determine new themes. The research approach was based on extracting views on the current NEC culture at a number of levels within each of the areas surveyed to provide a degree of vertical stratification. Such an approach was intended to establish the degree to which communication messages were being understood at various levels throughout the organization and the extent to which leadership behaviors were helping or hindering the adoption of the NEC philosophy. The data also provide opportunity to explore the range of perspectives from the military and civilian staff. Thereafter, the proposal is to use the validated research to gather further data via questionnaires and focus groups before providing an assessment of the gaps in skills, knowledge, and behaviors, and suggested ways of addressing these gaps.

Preliminary Findings

It is important to note at the outset that the themes that have emerged from the primary data gathering are indeed generalizations. Exceptions can be found within the MoD for every aspect reported in this essay The intention of highlighting the general themes is not intended as criticism but, rather, to help inform the MoD as to where additional effort needs to be placed if meaningful change in behaviors is to be embedded in the organization.

Training, Education, and Understanding

- Training and education underpin a great deal of the requirement, from ensuring that all staff have a basic awareness of NEC, to bringing all staff up to an adequate level of information

communication technology user skills and information management ability, to educating senior officers, training them on applications, and collective training before operational deployment. However, the overriding principle should be to develop an awareness of the rationale for and benefits of NEC over and above the skills involved in exploiting new technology and accompanying ways of working—the *why* as well as the *what* of NEC. A frequent comment about training was captured in the phrase, "we get buttonology without understanding." This is exacerbated by the increasing reliance on training in the workplace, either on the job or e-enabled, which meets with resistance because people feel that they are too busy and there is no discernible benefit to having completed the training.

- The technology is good, but people need to understand how to use it to best effect. People need to have trust and confidence in IT systems and processes. Not being able to email someone on a different system damages its credibility and users' confidence.
- Poor practice (e.g., sending documents rather than links and not sharing draft work) arises from both attitude and lack of familiarity with the technology.
- A total frustration with pathetic search engines arises, especially when you *know* that what you need is somewhere in the system.
- Knowledge of, familiarity with, and confidence in the equipment that people need to use will greatly enhance their ability to share, manage, and exploit information and operate effectively in a networked information environment. In addition, everybody needs to appreciate fully his/her responsibilities with regard to information sharing, management, and exploitation.
- Awareness of the benefits of NEC and the means of accessing information on the skills and attributes required to operate effectively in a networked information environment is limited. JSP 777 appears to be read only by those who believe that they need to as part of their professional responsibilities. In general, the perception is that NEC as a concept is overcomplicated and that it is either a preoccupation of specialists (front-line/communications experts/etc.) or an aspiration for the future. This aspect has major implications for the communications piece of delivering NEC.
- "Cynicism is a blocker, so don't give people grounds for being cynical."

- There is no formal training for captains and warrant officers (WOs), and the organization does not promote corporate memory.
- There should be officer military annual training tests (MATS) for NEC.
- What NEC means in the business space should be explained to make it real for civilians.

Leadership Issues

- There is an overall view that, because NEC is all-inclusive, leadership of the changes required to deliver it successfully must start at the top (VCDS/2nd PUS). It cannot be "parked" in any one area.
- "Traditional" style of leadership—command and control/face-to-face communications/decision-making, and so on—are generally well-regarded. Tactical leadership rates more highly than strategic/political leadership. Leaders need to be more open-minded and responsive and better at understanding, inspiring, and developing their staff.
- We need "charismatic" leaders—although the extent to which charisma can be taught/developed and leaders selected on the basis of their charisma is debatable.
- Leaders need to be aware of and acknowledge their lack of skills or knowledge, but this is seen as a personal failing in front of more junior personnel. Having the authority to command does not make a leader the subject matter expert. "Very bright people don't get air time because they aren't the right rank."
- Involvement of senior leadership in promoting required kit is getting better, therefore providing more interest and better direction, governance, and possibly funding for training.
- "You can't do leadership by e-mail." Leaders are needed who lead by example in NEC matters.
- Telling people the consequences of getting something wrong is less productive than explaining the benefits of getting it right.
- "I inspect units to see that the commander and the command chain drives the usage of joint personnel administration (JPA) and find, almost exclusively, that they are not."
- We have very competent leaders to deliver the "day job," but we lack strong inspirational leaders to lead and deliver change; thus, for NEC, we lack effective leadership.

Social Networks/Working With Others

- The development and maintenance of trust and confidence in a "social" relationship helps to enhance working relationships, particularly in the battle space. This becomes increasingly critical where dispersed teamworking and interoperability with non-U.K. Armed Forces organizations feature.
- "Developing effective relationships is the key to everything else."
- The tendency within the MoD (and elsewhere) to operate in stovepipes and to use "tribal" identities as a means of behaving (or not behaving) in a certain way can obstruct the successful delivery of NEC. This can be exacerbated when interoperating with other organizations and/or nations is required.
- The Army is not prepared to learn from anyone. For example, the Royal Navy and Royal Air Force have good JPA application, but the Army was never prepared to learn from them.

Acquisition Processes and Structures

- Acquisition processes need to begin with an accurate statement of requirement that is based on user needs rather than affordability or a perceived solution presented by industry. The processes also need to be sufficiently flexible to incorporate changing operational requirements and the need of the users to be involved in the development of equipment and capabilities—in short, a true partnering arrangement.
- Career pathways and double tours in key positions should be provided so that we can get some sort of coherence.
- People need a clear understanding of the capability acquisition process through training and education at a much earlier stage—in particular, those pursuing careers in the acquisition community should not be learning on the job when their focus is already on being credible and having an effect, and they are arguably less responsive to being educated about the why of NEC.
- The IPT construct is effective in managing all aspects of one program or project; however, it hinders the coherent acquisition of capability across the MoD to meet MoD needs.
- We are good at many things—including teambuilding, getting on and doing, working across boundaries if sharing a common aim— and these should be acknowledged and built on. Tribalism can be counterproductive, and there are numerous examples of services

competing against each other, for example in the acquisition of major new equipment.

Conclusion

We believe that elements within each of the themes are either repeated or expressed in slightly different ways, but it is clear that some fundamental change management lessons have emerged, and that failure to recognize and find solutions to these issues will invariably lead to a lack of progress on embedding an NEC culture.

Change management key lesson 1. It is necessary to communicate the need for change, and for this need to be expressed in a language that is meaningful to the target audiences. It was clear in the research findings that many interviewees had no real concept of what NEC meant to them, or indeed its relevance to their day job. The communication has to enable individuals to understand both the what and the why of change.

Change management key lesson 2. Where a change in behavior is required in the delivery of a capability, it is necessary to demonstrate the benefits of new behaviors through the provision of sufficient equipment and time to explore and practice, such that individuals can gain the necessary confidence in its use and can "see for themselves" the benefits of the new approaches and to confidence in them.

Change management key lesson 3. It is necessary for the organization to put in place systems and processes that can reward new behaviors being adopted to prevent individuals from defaulting to their old ways the moment the situation becomes difficult.

Change management key lesson 4. Leadership needs to start from the "top of shop" and be seen to be leading by example. If new behaviors are required as part of the culture change, then the leadership at all levels needs to take ownership of the challenges and needs to be seen to be adopting and supporting new behaviors.

Change management key lesson 5. Management in general needs to recognize that to bring about lasting change, some of the systems and processes in the current organization will need to change in fundamental ways. For example, the acquisition

process needs to reflect that equipment and systems users in the future will behave in very different ways, and that the new capabilities need to be designed with this in mind. It cannot be the case that we procure future systems that look and feel the same as the current ones, as this will only serve to reinforce current practices and behaviors. To achieve this one aspect concerns a change in philosophy to one of "what do we need?" as opposed to, "what can we afford?"

Change management key lesson 6. This is probably the most important of all of the lessons, in that it requires the leadership and the organization to recognize that appropriate investment and time need to be devoted to the people dimension of change and that it should not be the defense line of development (DLOD) that is picked up at the last moment. Failure to recognize this will inevitably result in systems and capabilities that are introduced but fail to deliver their full potential or find themselves being modified from day one in a continual effort to make them workable for those who have to use them.

Innovation in the people dimension is certainly possible through the use of technology, and this opens the door for a more creative use of simulation and synthetic environments. However, the approach to the use of technology needs to be challenged. At present, we tend to use it as a training tool to give individuals and groups practice at using applications before deployment or as part of officer broader education. It is our view that to effect cultural and behavioral change, the MoD needs to use the power of technology to challenge the current systems and processes. In other words, it should not be about simply improving efficiency in the current paradigm but about challenging the paradigm itself to be more effective. To this end, battle labs have a role to play when used in the context of challenging behaviors and as a basis for developing better understanding of the social interactions necessary to deliver the full benefits of networked decision-making. Away from the operational context, there also exists scope to use examples such as the "model office projects" to explore how individuals and groups might be able to interact in better (more effective) ways, such that the quality of output from individuals and groups—and hence the organization—might be improved. It must be recognized that this is about far more fundamental change than simply doing today's business more

efficiently—that a change in paradigm is required if the organization is to make a step change in its performance.

Aligned to innovation in technology and its exploitation is the need for innovation in behaviors and culture, not least in the approach to leadership in the MoD. Although there is a need for a highly directive and autocratic style of leadership on operations, it is clear that this is becoming increasingly less productive and appropriate away from the front line. Indeed, one could argue that in an increasingly technology-driven military, there must be a clear distinction drawn between decision-making—which is entirely the responsibility of the leader—and the various leadership processes and attributes and support functions that must be present to enable decisions to be taken. There is a clear need for leaders to be innovative in stepping away from a traditional, hierarchical approach in which rank confers authority without question and toward a flatter approach in which the skills and attributes required to support the leader's decision-making ability are clearly and precisely identified and accessible, regardless of rank or service and without there being any question that this consultative approach will bring about an unacceptable shift in the balance of authority. Both on operations and away from the front line, it is essential that leaders understand the people in their teams, but it is no longer enough to be aware of their skills and experience; particularly where they are leading dispersed or virtual teams, as is increasingly the case, they must understand individuals' personalities, what drives and discourages them, and what they expect of their leaders, and they must also trust these leaders to fill the skills and knowledge gaps appropriately.

In turn, individuals expect their leaders to be courageous and inspiring in their leadership, but in this day and age, this often means acknowledging that they do not have all the answers and allowing their subordinates to take risks and learn from mistakes while managing the effects of those mistakes, focusing attention on a clear outcome, and putting their people through some degree of discomfort to get there. Leaders must be able both to explain why a particular course of action (or change initiative) has not been successful and deliver the unpalatable message that an unpopular course of action (or change initiative) must be pursued to enable achievement of a necessary goal.

In terms of individuals, there appears to be within the MoD an increasing aversion to taking risks and allowing others to take risks, which may well stifle the innovation and creativity necessary to deliver

NEC successfully. There appear to be several reasons for this, including a blame culture that begins above departmental level, a reliance within the military on getting a good confidential report at the end of a posting for career progression reasons, and the key role of the media in broadcasting information on military activities on operations and elsewhere. Individuals must be able to challenge those in authority if they believe that to do so will benefit the greater good and if they do so in a constructive way it will not threaten their career prospects. This is uncomfortable for both subordinates and leaders because both will fear the consequences to them personally of behaving in this way. To do so requires mutual trust and respect and a full awareness of others' abilities and personalities, which are behaviors necessary to achieve NEC. Not to do so, however, risks failing to exploit the full power of the networks and the technology available, which is unacceptable in the NEC era. Courageous followership is becoming as important as courageous leadership, and a key role of leaders should be to develop courageous followers to go on to become courageous leaders in their turn.

In support of this, the authors believe that creativity needs to be applied to generate case studies and scenarios that provide clear evidence that the adoption of new behaviors is beneficial to both the individual and the organization. A very simple example of this concerns the behavior of sharing information as opposed to hoarding information. Although most people will be able to understand the benefits from a cognitive perspective and will subscribe to the approach, that is not the same as defining how they will behave in a range of pressure situations. Such behavior has not been embedded into their psyche, and they run the risk of reverting to type. Sharing information is about far more than the technology or the orders that you are following. If it is the case that deep down, one feels that having control of information is an issue of power and influence, or a sense that you own the information, then the embedded behavior is one of having the right to determine "who gets what where and when," and of others being grateful to have received it. However, from a cultural and behavioral perspective, this is very different from seeing yourself as one who can help others to make better informed decisions to the benefit of all concerned. In this context, instead of being the controller of a resource, one sees the sharing of information as a means to enable others to make better, timelier, and more confident decisions.

It is also the case that technology can be used in more innovative ways to communicate the intent of the change. The current practice of dumping "stuff on the Intranet" or firing out communications in newsletters is alright at a superficial level, but in terms of delivering key change messages, it generally does not achieve the objectives from the point of view of those in the organization who need to have a much deeper understanding of what is expected of them. A much richer array of communication is required; this also falls to the role of leadership in "walking the walk," rather than issuing pronouncements.

References

Bechky, B. (1999). Cited in Sole, D. & Edmonson, A. (2002). "Situated Knowledge and Learning in Dispersed Teams," *British Journal of Management*, 13, S17–S34.

Chidambaram, L. (1996). "Relational Development in Computer-Supported Groups," *MIS Quarterly*, June, 143–161.

Cramton, C. (2001). "The Mutual Knowledge Problem and Its Consequence for Dispersed Collaboration," *Organisational Science*, 32, 554–571.

Gibson, C. & Cohen, S. (eds.) (2003). *Virtual Teams That Work: Creating Conditions for Virtual Team Effectiveness*. San Francisco, CA: Jossey-Bass.

Hamel, G. & Prahalad, C. (1996). *Competing for the Future*. Boston, MA: Harvard Business School Press.

Jarvenpaa, S. & Leidner, D. (1999). "Communication and Trust in Global Virtual Teams," *Organisational Science*, 10(6), 791–815.

Jones, G. & George, J. (1998). "The Experience and Evolution of Trust: Implications for Co-operation and Teamwork," *Academy of Management Review*, 23(3), 531–546.

Looy-Hyde, J. (2007). "Dispersed Teamwork: Leadership, Communication and Relationship Building Through Technology," DSTL working paper. DSTL/WP24162

Meyerson, D. et al. (1996). Cited in Jarvenpaa, S. & Leidner, D. (1999). "Communication and Trust in Global Virtual Teams," *Organisational Science*, 10(6), 791–815.

Neal, D. & Taylor, T. (2006). "Spinning on Dimes: The Challenges of Introducing Transformational Change Into the UK Ministry of Defence," *Strategic Change Journal*, 15(1), 15–22.

Neal, D. (2007). "Incorporating the Human Factor in Delivering Change: The Case for NEC," Transformation and NCW/NEC Conference, Geneva, September 25–26.

Sonnenwald, D. et al. (2004). "Designing to Support Situation Awareness Across Distances: An Example From a Scientific Collaboratory," *Information Processing and Management*, 40, 989–1011.

Walther, J. & Burgoon, J. (1992). Cited in Pauleen, D. (2004). "An Inductively Derived Model of Leader-Initiated Relationship Building With Virtual Team Members," *Journal of Management Information Systems*, 20(3), 227–256.

Warkentin, M. et al. (1997). "Virtual Teams Versus Face to Face Teams: An Exploratory Study of a Web-Based Conference System." *Decision Sciences*, 28, 975–996.

Essay 4

Transforming Interagency Education

People and Process Requirements for Success

By Ralph Doughty and Terry Pudas

Abstract

Many studies have been conducted and speeches delivered about the need for a "whole of government" approach in the use of combined soft and hard power within governmental departments and agencies. Multinational forces and nongovernmental organizations are also needed to create a "comprehensive approach" for use in stability operations, disaster response, and humanitarian assistance missions.

A solution to this dilemma is to educate and train all organizations involved so they understand each other's capabilities and constraints before they deploy together for operational assignments. Because of people and funding constraints, most agencies are extremely reluctant to participate in long-term education and training programs. To address these needs, the U.S. Army created a new exchange program to enable agencies to send their employees as students to the U.S. Army Command and General Staff College, and for participating agencies to sponsor Army officers to serve as interagency fellows at their agencies.

This transformational solution involved people and process changes that required decision-makers in the agencies and the Army to first recognize the need and then modify their processes to enable interagency personnel to participate. This was accomplished successfully, and the pilot program is now being institutionalized within the Army.

Introduction

Many studies and speeches have been written about the need for a "whole of government" approach to the use of soft and hard power within government departments and agencies. As we strived to create a joint military force in the 1980s, we created new structures and processes. Ultimately, we understood that our ability to function as a truly joint force hinged on creating a new culture—a joint culture. With great effort, some pain, and help from Congress, we set about creating the joint professional military education program. Incentives were put in place making promotion of senior officers to flag and general officer rank contingent on completion of joint education and joint assignments. Over more than 20 years, a truly joint force evolved, one capable of bringing all elements of Department of Defense (DOD) capabilities to bear in an integrated and interdependent way. The initial phase of Operation *Iraqi Freedom* suggests that changing culture and behavior, although neither quick nor foolproof, can yield dramatic returns.

We are at a point similar to the early 1980s, but on a much grander scale, in which the consequences of failure are too grave to contemplate. Clearly, there is a need for a larger and more cohesive team embracing all elements of national security. To bring to bear all the capabilities needed to prevail over the irregular, disruptive, and potentially catastrophic challenges facing us will require unity of effort and unifying institutions.

Multinational forces and nongovernmental agencies are also needed to create a "comprehensive approach" that is capable of operating effectively in stability operations, disaster response, and humanitarian assistance situations anywhere in the world. Good progress is being made in integrating civilian and military personnel into organizations that bring together the best qualities of each agency or service to create an organization that is tailored to the specific mission of the combined organization. One example of this is the development of provincial reconstruction teams (PRTs) to address stability and reconstruction in environments that are unstable or dangerous, such as in Iraq or Afghanistan. First used in Afghanistan in 2002, a PRT is a military/civilian unit that assists with security, stabilization, and reconstruction efforts in unstable nations and complex environments. Other examples focus on agriculture to identify ways to improve the productivity of farmers and assist them in the selection of legal crops

that can provide increased cash flow to support themselves and their local villages or provinces. As of March 2008, there were 26 PRTs in Afghanistan and 28 in Iraq. Critics of the programs note that the different agencies, funding sources, and authorities may lead to a lack of program coherence, or that they lack clear lines of authority, agreed missions, and measurable objectives.

Creation of joint interagency coordination groups (JIACGs) is a relatively new initiative to coordinate U.S. Government civilian agencies' operational planning in contingency operations. A JIACG supports day-to-day planning at the combatant commander headquarters; advises planners regarding civilian agency operations, capabilities, and limitations; and provides perspective in the coordinated use of all elements of national power. Functionally, JIACG tasks include working civil–military campaign planning issues and conducting outreach to key civilian international and regional contacts. Operational JIACGs have been established at all regional combatant command headquarters, although composition, organizational structure, and effectiveness vary.

Another recent creation is the Center for Complex Operations (CCO), a DOD-led collaborative effort with the Department of State and the U.S. Agency for International Development (USAID). The CCO defines complex operations to include counterinsurgency; stability, security, transition, and reconstruction operations; and irregular warfare.[1] The CCO is developing a community of practice of civilian and military complex operations training and educational institutions and practitioners. The goal of the CCO is to enhance the ability of the U.S. Government to prepare for complex operations by catalyzing cooperation, coordination, and synchronization among educational, training, lessons-learned, and research institutions and organizations.

On February 6, 2007, President George W. Bush and Secretary of Defense Robert Gates announced the creation of U.S. Africa Command (USAFRICOM), an organization that enables DOD to better focus its resources on existing U.S. development and security initiatives in the region and provides African nations and regional organizations an integrated DOD coordination point to help address related needs. USAFRICOM is intended to build a more integrated staff structure, one that includes significant management and staff representation by the

---

[1] OTHERS ….

Department of State, USAID, and other U.S. Government agencies involved in Africa. This is a major departure from the typical DOD military command structure and reflects an understanding of the key relationships among security, development, diplomacy, and prosperity in Africa.

All of these "comprehensive approaches" involve placing people into environments that are new to them, such as the addition of State Department or Department of Agriculture personnel to a military organization operating in a reconstruction and stabilization environment. This structure results in players from the various organizations suddenly finding themselves in a new mission with partners they have never met whose methods of operation they do not understand. This clearly leads to inefficiencies and wasted motion that are sometimes dangerous and invariably delay the accomplishment of the mission.

In an effort to integrate the total force with senior military and civilian professionals throughout all branches of the U.S. Government, the 2006 Quadrennial Defense Review describes DOD support for the creation of an interagency National Security Officer Corps. DOD also is looking to transform the National Defense University to better support the education of U.S. national security professionals.

A solution to this problem is to educate and train all organizations involved so that they understand each other's capabilities and constraints before they deploy together. This "joint" education and training is one of the key tenets in Presidential Executive Order 13434 (Bush, 2007), which implements a national policy to develop a cadre of trained national security professionals in executive departments and agencies. Although this solution makes sense, problems immediately arise when the various departments and agencies involved realize that they have neither the people nor the funding to enable them to send employees away for education and training. Most Federal departments and agencies are a monolayer deep in their staffing levels, and if they send someone off to training, the job that individual is assigned to do simply does not get done. In addition, money is extremely scarce in most departments and agencies, so funds are rarely available to send employees to education and training programs. As a result, departments and agencies are extremely reluctant to participate in education and training programs.

DOD recognizes that it is in the best interest of both the services and the civilian agencies with which they share responsibilities to find a

way to solve this problem. Secretary Gates has repeatedly stated that the military does not want to take over the missions of other departments and agencies, preferring to work in a coordinated fashion with them to develop a more robust capability within them so that more effective teamwork could take place to get the missions accomplished. In remarks at the Brookings Institution on May 5, 2008, Secretary Gates said, "the State Department must be strengthened even further— in money, people, and bureaucratic clout—to truly fulfill its responsibilities as the lead agency in American foreign policy" (Gates, 2008). This is easier said than done, however. Transformation of long-standing traditions and methods is difficult to achieve and normally requires a real sense of urgency for change, a vision for how the transformation should be accomplished, and a powerful guiding coalition to lead the implementation (Kotter, 2005).

A New Approach

Based on strong leadership from the top, the U.S. military has begun to make the transformation to a more comprehensive approach to dealing with situations requiring involvement of whole-of-government as well as nongovernmental agencies and multinational participation. A number of initiatives are currently underway to transform old stand-alone approaches to a comprehensive approach that includes all appropriate government and nongovernmental players. One of these initiatives is being led by the U.S. Army Command and General Staff College (CGSC), a subordinate organization of the U.S. Army Combined Arms Center at Fort Leavenworth, Kansas, which has developed a new program called the CGSC Interagency Exchange Program. This is a two-part program in which various agencies are invited to send their employees as students to participate in a variety of CGSC educational programs, and participating agencies sponsor CGSC interagency fellows to work in their organizations to provide broadening experiences for the army personnel.

The Department of the Army officially authorized the Training and Doctrine Command to pilot this program on May 5, 2008. The first round of the Pilot Program, which was conducted in cooperation with the Army Human Resources Command during academic year 2009, is now complete and resulted in 24 students for CGSC from eight departments and agencies. In addition, seven CGSC interagency fellows were placed with six agencies. Participating departments

and agencies included Department of State (Main), Department of State Office of the Coordinator for Reconstruction and Stabilization, USAID, Defense Intelligence Agency, Central Intelligence Agency, National Geospatial-Intelligence Agency, Federal Bureau of Investigation, Department of Health and Human Services, and the Veterans Administration.

Current projections for academic year 2010, which began in the summer of 2009, indicate a total of about 35 interagency students from 14 departments/agencies with 21 CGSC interagency fellows planned with 13 agencies, which—in addition to the departments and agencies mentioned earlier—now include the Department of Homeland Security, Department of Justice, Defense Threat Reduction Agency, Department of the Treasury, and Department of Agriculture. These exchanges provide a forum in which military and interagency personnel can learn and appreciate the capabilities each brings to the problems at hand, which results in experiential learning gained by working issues side-by-side in an educational environment that is similar to the operational environment they will face together in stability operations, disaster response, or humanitarian assistance missions.

This transformational solution had significant hurdles to leap before it could be successful. First was the transformation of the people who make decisions on the composition of classes that make up the curriculum. Many decision-makers saw no need for civilians to be allowed into the classes at all, feeling that they displaced army officers from seats that were rightly theirs. Once these decision-makers were given enough information to finally "see the light," the next step was to modify the processes that governed the conduct of the courses and to include interagency needs and constraints into the exercises that were part of the curriculum. Fortunately, the technology had been designed and built into the CGSC Lewis and Clark Center to enable these changes to be made expeditiously.

The CGSC Interagency Exchange Program is now in its second year, and benefits are already being realized. One organization, USAID, had two of its civilian employees graduate from the program in the summer of 2008. One of these graduates is now the USAID representative on the staff of the U.S. Central Command and is participating in their assessment of the stability of various countries and regions of the world. The other graduate is now in Afghanistan working in Combined Joint Task Force 101, where they are beginning to see progress in dealing with the real-world problems that exist there.

Clearly, this joint program of education and training with all interagency players is beginning to pay dividends for all parties involved, but that is not the end of the story. Not only are the students increasing their skill levels and learning to operate over a broader spectrum of challenges but the Army and the various agencies are gaining new perspectives that translate into increased capabilities for joint operations. So this part of the program has been successful in transforming the "normal" way of doing business separately into a team effort in which the players understand each other's capabilities and constraints, thereby resulting in a more responsive and capable team that can deploy and immediately begin to identify and implement workable solutions.

Again, however, this is not all. The second part of the CGSC Interagency Exchange Program enables U.S. Army officers, typically majors who have already completed the CGSC Intermediate Level Education course, to serve a fellowship in the departments and agencies that send students to study at CGSC. This fellowship allows the Army officers to work alongside agency employees in the agency setting, which results in a tremendously broadening experience for these fellows. Separate papers are being written by these fellows to describe the types of assignments in which they have been involved in their individual agencies. Assignments to date have included participation in the development of diplomatic responses to the Georgia crisis in 2008 and an on-the-ground assessment in 2009 of methods for improving the value of geospatial intelligence supplied to U.S. troops in military operations.

The Way Forward

The ultimate solution is for the Obama Administration and Congress to see the benefits of fully integrated education and training and provide adequate funding to the civilian departments and agencies to enable them to participate with the U.S. military at the levels needed to generate educated and fully trained teams to take on the tasks in front of us throughout the world. With more successes like the ones seen so far in the CGSC Interagency Exchange Program, this is viewed as a distinct possibility. As a matter of fact, a number of key leaders are advocating laws to more fully integrate departments and agencies into a better-educated and better-trained team capable of working more effectively with their international partners and nongovernmental

organizations by developing a national security career path for civilian professionals similar to the Joint Service Officer model in the military (Flournoy & Brimley, 2008).

One solution would be legislation to bring about the same type of joint actions for the interagency that were experienced in the original Goldwater-Nichols Law, which created the Joint Force of all the military departments (Locher, 2008). The difficulties of operating in a joint, interagency environment today are many, and the solutions will likely require legislation that overhauls the entire national security system. However, that is not the purpose of this essay. Rather, the purpose of this essay is to identify and describe methods that can successfully integrate the education and training of national security professionals to create a more functional comprehensive approach as we move toward increased interagency cooperation. The following sections describe the changes in people and processes that are necessary to achieve this improved educational and training environment.

People Changes

The first change required is that people involved in joint education of national security professionals must recognize the fundamental need for joint education and training. People cannot cooperate with other organizations effectively without first understanding the capabilities and constraints of their own and the other organizations. This requires education and collaboration with the other organizations. When people "don't know what they don't know," it is difficult for them to see the need for more education and training. As a result, employees are not inclined to volunteer for additional education or training unless they are directed to do so by their superiors. One way to address this problem is for organizations to first get their senior leaders on board with the need for education, and then for those senior leaders to implement personnel policies that reward employees for getting the right education and training. That is, education with departments and agencies outside their own are then viewed as "career-enhancing assignments" that result in better jobs and more responsibility for the employees who obtain the joint interagency education and training. This will then lead to a change in the culture of the organization that will fundamentally transform the way employees think and act about joint interagency education.

The people who are senior leaders must also transform the way they communicate to subordinates. It is not good enough for an agency to release a notice of the availability of educational and training programs their employees may want to attend. Simply releasing this notice without first creating and implementing human resources programs that specify the benefits to the employees for selecting these educational programs (which clearly require work and entail hardship to complete) will not yield positive results. Personal involvement with high-potential employees is one good way to send the message to others in the organization that getting interagency education and training is a good way to enhance a career.

Human resource staff must also work to ensure that the monetary costs of gaining added education and training do not fall on the shoulders of employees. Travel and temporary duty costs must be adequately funded by the department or agency, as the employee is already sacrificing by moving family or by being away from them for extended periods of time to get the added education.

Process Changes

A number of process changes are needed to implement an effective joint education and training program in the interagency. First is the recognition that a "schools account" or "personnel float" is needed so that the organization's work output does not suffer while people are away at school. This Schools Account does not exist in most departments and agencies—hence the need for the CGSC interagency fellows, who are able to come into the departments or agencies sending students to CGSC and help to limit any reduction of work output from the agency. In reality, however, this could be considered as a short-term solution that helps until the departments and agencies can gain adequate funding and personnel authorizations to create their schools account and handle it themselves. Until this point is reached, however, the use of army officers as CGSC fellows to the individual agencies is essential, and also provides a much-needed learning and broadening experience for the fellows, who will then be much better prepared to work in operational interagency assignments in the future. For this reason, it may be that "never" is the right time to cease the assignment of fellows to departments and agencies.

Second, appropriate selection processes need to be developed and put into place in the agencies to enable the most deserving employees

to be selected for needed education and training. These processes should be based on the fundamental premise that such selection is a career-enhancing assignment, and that not only will their employees come back from their schooling better prepared to serve in joint interagency assignments, but they will be much more likely to get assignments that further their careers. Once this process is clearly in place in the organization, there will not be problems with finding volunteers for education and training opportunities.

Processes must also be in place to routinely reimburse the employees fairly when they must travel and live for a time away from their normal place of work. This requires senior-level leadership at the start, and then it requires that processes continue to ensure that this is routinely accomplished.

One of the key processes in the CGSC Interagency Exchange Program is that the interagency personnel who come to CGSC are placed in small, 16-person seminar groups, where they receive most of their education. These seminar groups have a carefully coordinated mixture of combat and combat support officers from the Army, as well as one or two joint service officers from the Air Force, Navy, or Marine Corps, and an international officer from one of over 80 countries. The objective of the CGSC Interagency Exchange Program is to also include one interagency student in the staff group. With this type of student mix, a range of joint, international, and interagency perspectives is included in the class discussions and group exercises. As a result, excellent experiential learning occurs that would be almost impossible without this mix of highly knowledgeable and experienced officers and civilians, who learn cultures and methods of operating with their joint/interagency counterparts on a daily basis. Finally, personal relationships are developed that will last for a lifetime of personal and professional successes. The combination of these processes and the multicultural perspectives experienced by the students on a daily basis results in extremely well educated students who are prepared for the complex and uncertain challenges they must face together in the future.

The final process change that is critical is to develop innovative ways to overcome the lack of money and people so as to be able to accomplish these educational and training initiatives. The exchange program is clearly one innovation that helps to defray costs and encourage people to participate. Many more methods are needed, however, as we will never have all the money we need to educate and train everyone to the levels we wish.

Conclusions

Old habits die hard, and transformation is often thought to be a gimmick used by senior level personnel to acquire additional funding, power, or prestige. However, whether through new technology, processes, organizations, or innovations, mankind has always found new and better ways to fight. With the resurgence of irregular warfare and the problems associated with instant information availability to virtually everyone in the world, we must not forget that educated teams of all the organizations available to a country are needed if we are to be successful.

Joint education for our military leaders has paid enormous dividends. It is imperative that we explore the creation of a similar construct for the leaders of agencies and departments responsible for prevailing over current and future security challenges. The United States runs the risk of squandering its economic, informational, military, diplomatic, and technological advantages unless we invest in our most valuable commodity—our future senior leaders—to create the attitudes, values, and beliefs that underpin a new culture. This is a matter not of cost but of choice and is fundamental to our future success.

This essay has described one way to provide the needed education and training by exchanging people who can help to educate each other and change the culture of the participating organizations. This transformational solution involved people and process changes that required decision-makers in the agencies to first recognize the need and then modify processes to enable interagency personnel to participate. Changes to internal army processes were also required to provide interagency fellows to serve in the agencies. This was accomplished successfully, and the pilot program is now being institutionalized within the U.S. Army, with exceptionally valuable results for the organizations and nations involved.

References

Bush, G. W. (2007). Presidential Executive Order 13434, National Security Professional Development. Washington, DC, May 17.

Flournoy, M. & Brimley, S. (2006) "In Search of Harmony: Orchestrating 'The Interagency' for the Long War," *Armed Forces Journal*, July.

Gates, R. (2008). Remarks to the Board of the Brookings Institution. Washington, DC, May 5.

Kotter, J. (2005). "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review*, Winter.

Locher III, J. (2008). "The Most Important Thing: Legislative Reform of the National Security System," *Military Review*, May–June.

Essay 5

Transformational Initiatives in Civil–Military Operations

STAR-TIDES and Maritime Environments

By Linton Wells II and Walter L. Christman

Abstract

The Department of Defense is increasingly involved in missions such as post-war stabilization and reconstruction, humanitarian assistance/disaster relief, and building the capacity of partner nations. An international, knowledge-sharing research program called STAR-TIDES examines innovative approaches to public-private collaboration and "whole-of-government" solutions to provide affordable, sustainable support to stressed populations in these environments. STAR-TIDES encourages unity of effort among diverse organizations where there is no unity of command. It addresses problems through seven broad action areas:

- *Gather, share, and evaluate information about capabilities*
- *Develop social networks and build trust*
- *Align policy, doctrine and field operating procedures*
- *Resolve legal and regulatory constraints*
- *Address resource requirements*
- *Train, exercise and educate, and*
- *Integrate with associated activities.*

Implementing these measures requires crosscutting changes among people, processes, operations, and technology in complex, civil-military environments that are every bit as transformational as high-end warfare initiatives. STAR-TIDES approaches have been examined extensively in terrestrial contingencies, but not yet in maritime ones. This paper focuses on their application to maritime environments and their effects on the Sea Services.

Introduction

National security transformation seeks major advances in capabilities for defense, diplomacy, and development through changes in people, processes, organizations, and technology. It is an ongoing process, not a finite event. This essay examines some aspects of transformation by investigating interactions between two initiatives, the 2007 Maritime Strategy and a research project called STAR-TIDES.[1] It emphasizes activities that involve more than one of the transformation categories, such as how people interact with processes, or technology with organizations.

A Cooperative Strategy for 21st Century Seapower was issued jointly by the Chief of Naval Operations, the Commandant of the Marine Corps, and the Commandant of the Coast Guard in October 2007.[2] It is a seminal document and a significant departure from past approaches. The new Maritime Strategy moves beyond traditional naval roles such as power projection, sea control, strategic deterrence, and forward presence to include capabilities like maritime security, humanitarian assistance, and disaster response. This embraces evolving notions of cooperative security,[3] which the strategy explores in depth, promoting interoperability and engagement with diverse partners.

One of the strategy's central tenets is that "Preventing wars is as important as winning wars" which reflects the fact that the Department of Defense (DOD) is increasingly involved in missions such as postwar stabilization and reconstruction, humanitarian assistance/disaster relief,

---

[1] TIDES stands for Transformative Innovation for Development and Emergency Support. TIDES is part of a broader effort, Sustainable Technologies, Accelerated Research, or STAR. Hence, STAR-TIDES.

[2] Chief of Naval Operations, Commandant of the Marine Corps, and Commandant of the Coast Guard, *A Cooperative Strategy for 21st Century Seapower* (2007), Introduction.

[3] See, for example, Commander, U.S. European Command and Commander, U.S. Joint Forces Command, *Military Contribution to Cooperative Security*, Joint Operating Concept, version 1.0, September 19, 2008. It defines cooperative security as, "The set of continuous, long term, integrated, comprehensive actions among a broad spectrum of U.S. and international governmental and nongovernmental partners that maintains or enhances stability, prevents or mitigates crises, and enables other operations when crises occur." A more theoretical treatment is provided by Michael Mihalka, "Cooperative Security in the 21st Century," *The Quarterly Journal* 2005(Winter):113–122.

and building the capacity of partner nations. It also mirrors the profound changes that have taken place in U.S. national security strategy, policy, and doctrine since 2004.[4]

The new Maritime Strategy is complemented by an innovative, international social network focused on knowledge-sharing that is part of the STAR-TIDES project.[5] The project examines transformational approaches to public–private collaboration, whole-of-government solutions, and transnational engagement. It is pioneering new forms of global partnership, with a goal of providing sustainable, affordable support to stressed populations in postwar, postdisaster, or impoverished environments. STAR-TIDES encourages unity of effort among diverse organizations where there is no unity of command. Combining distributed organizations and new institutional approaches to cooperative security can improve effectiveness in complex, civil–military environments. Such efforts may be every bit as transformational in the prevention of war as advanced research and development and high-performance systems procurement are in the preparation for combat operations.

STAR-TIDES approaches have been examined extensively in terrestrial contingencies,[6] but not yet in maritime ones. This essay thus focuses on the approaches' applicability to maritime environments, their transformational aspects, and their effects on the Sea Services. It links theory and practice to highlight ways in which the new Maritime Strategy can flourish in the context of diverse, crosscutting initiatives that link people, processes, organizations, and technology in novel ways.

---

[4] The National Security Strategy and National Defense Strategy address complex operations and engagement with civilians; DOD Instruction 3000.05 focuses on Stability Operations; Army Field Manuals 3-0 (Operations), 3-07 (Stability Operations) and 3-24 (Counterinsurgency, which also is Marine Corps Warfighting Publications 3-33.5) provide Service-level doctrine on these types of situations.

[5] TIDES = Transformative Innovation for Development and Emergency Support. It is part of the broader effort called STAR (Sustainable Technologies, Accelerated Research).

[6] See, for example, Linton Wells II et al., *STAR-TIDES and Starfish Networks: Supporting Stressed Populations with Distributed Talent* (Center for Technology and National Security Policy, Defense Horizon, 2009, forthcoming).

The Maritime Strategy

This essay addresses two questions: How can the distributed organizational structures represented by STAR-TIDES help meet the goals of the Maritime Strategy? And how are these structures transformational?[7] Can examples of cooperative security with nontraditional partners be used to illustrate links between new organizational forms and the goals of the Maritime Strategy?

The Maritime Strategy is shaped by the proximity of large populations to the coast worldwide, along with disruptive factors such as social instability, the effects of climate change, mass communications that focus on human suffering, and extremist and criminal elements that arise as a result of instability. To counter these emerging threats, the Maritime Strategy seeks to integrate sea power with:

> other elements of national power, as well as those of our friends and allies. It describes how seapower will be applied around the world to protect our way of life, as we join with other like-minded nations to protect and sustain the global, inter-connected system through which we prosper. Our commitment to protecting the homeland and winning our Nation's wars is matched by a corresponding commitment to preventing war.

This requires global cooperative engagements among governments, nongovernmental organizations (NGOs), international organizations (like the United Nations), and the private sector, all partners with whom STAR-TIDES seeks to engage as well. The Maritime Strategy's focus on reducing the causes of instability also aligns with STAR-TIDES' focus on reducing stress on populations.

This emphasis on interdependency—a recurring theme of the Maritime Strategy—represents a major conceptual change from the way sea power was envisioned only a few years ago. It occurs within an emerging cooperative security concept that moves beyond deterrence based on conventional and nuclear warfighting capabilities as the primary means of preventing war. Although by no means abandoning the need for decisive combat power, the strategy recognizes that U.S. security interests are linked with those of other

---

[7] The authors wish to thank Ivan Labra, a research associate at the Naval Postgraduate School, for posing the issue in this insightful way and for his thoughts in addressing it.

nations and emphasizes the importance of engaging effectively with the world's interlocking "networks of trade, finance, information, law, people and governance." It fosters asymmetrical global partnerships to address emerging challenges to human security posed by globalization and climate change.[8]

The U.S. approach is not unique, however, as innovative navies around the world are focused on similar transformations. Rear Admiral Tan Kai Hoe, Chief of Staff of the Singapore Navy, outlines the issues well:[9]

> While different navies may face different specific challenges, there are some global trends which are key drivers of transformation. Chief amongst these is the uncertain global environment, with an increase in new security threats and security concerns . . . in addition to fulfilling their traditional roles of ensuring good order at sea and protecting maritime commerce, [navies] are also expected to contribute towards the maintenance of global security through ensuring maritime security against terrorism, or by standing ready to provide relief to natural disasters. [Navies also] must continue to hone a sharp edge in conventional war fighting to deter aggression, and to win in conflicts if necessary. [T]hey have to develop new capabilities, structures and processes to meet the broadened range of new and existing operational demands.

A key tenet of the Maritime Strategy is to foster cooperative relationships over time, which means the Sea Services must develop more expertise in the cultures, histories, and languages of international partners. They also must coordinate better with other U.S. armed forces and government agencies. As the strategy says:

> Although our forces can surge when necessary to respond to crises, trust and cooperation cannot be surged.[10] They must be built over

---

[8] The Maritime Strategy relies on six core capabilities: forward presence, deterrence, sea control, power projection, maritime security, and humanitarian assistance and disaster response.

[9] Tan Kai Hoe, RADM, "Naval Transformation: Progress, Prospects and People," *Pointer: Singapore: Journal of the Singapore Armed Forces* 2008;34(2):6. It is noteworthy that Singapore entrusts roughly 1 percent of its defense budget to the "Future Systems Architect," charged with developing transformational concepts.

[10] STAR-TIDES-related research into human interoperability is looking at ways to accelerate trust-building across different cultures. It clearly is better if trust has been built and social networks developed before a crisis emerges, but

time so that the strategic interests of the participants are continuously considered while mutual understanding and respect are promoted.

Forward maritime deployments help promote sustained relationships with partners, enable rapid responses after disasters, and help mitigate disruptions or keep them localized.

STAR-TIDES and the Maritime Strategy: Three Dimensions of Interaction

STAR-TIDES can complement the Maritime Strategy by helping to create more stable environments and reduce preconditions for conflict.[11]

In lieu of the deployable, expensive, and hard-to-sustain types of equipment that DOD often brings to these contingencies, STAR-TIDES focuses on crosscutting, whole systems[12] approaches to seven types of infrastructures: shelter, water, power, integrated combustion and solar cooking, cooling/lighting/heating, sanitation, and information and communications technologies. STAR-TIDES supports the rapid dissemination and adaption of knowledge developed in these domains though the use of online collaborative capabilities and the creation and maintenance of publicly available knowledge repositories through its Web presence at http://www.star-tides.net.

The STAR-TIDES concept cultivates interactions among nontraditional partners. Joining STAR-TIDES' adaptive capabilities to the capacity of our maritime organizations and their international

---

it may be possible to build trust more quickly than expected, even under stressed conditions. Research is ongoing.

[11] Three specific areas of emphasis outlined in the Maritime Strategy lend themselves to STAR-TIDES-like interactions: improve integration and interoperability, enhance awareness, and prepare our people. In addition, the Capstone Concept for Joint Operations (CCJO), signed in January 2009 by the Chairman of the Joint Chiefs of Staff, identifies four basic categories of military activity for the Joint Force in 2016 to 2028: combat, security, engagement, and relief and reconstruction. STAR-TIDES contributes directly to the last two categories and indirectly to setting the conditions for security.

[12] "Whole systems" in this context means looking at approaches among different infrastructures to see how they can complement each other. For example, heat from solar cooking can purify water and also heat rocks or bricks to help avoid pulmonary and eye diseases from having to burn fires inside shelters.

partners could be transformative—a "non-force" multiplier, if you will. It helps establish the conditions for peace.

The transformational nature of STAR-TIDES' organizational construct lies in its ability to access distributed talent. It leverages new technologies to create on-demand, resilient capabilities that are focused, yet broadly accessible and comprehensive. Drawing on this, STAR-TIDES can interact with traditional maritime approaches along three dimensions:

- provide **crosscutting analyses** of capabilities for distressed populations that apply to the seven core TIDES infrastructure areas;
- promote rapid **process innovation** to improve ways of doing business in such areas as unclassified information sharing; and
- assist in **developing and implementing partner-centric solutions** through an agile planning process that engages public–private, whole-of-government, and international partners. This approach contributes to unity of effort among diverse organizations that will not subordinate themselves to a single chain of command.

The global talent accessed by the STAR-TIDES network has helped address real-world problems such as stabilization and reconstruction in Afghanistan, humanitarian assistance/disaster recovery (HA/DR) in tropical regions such as Cyclone Nargis relief in Myanmar, and building the capacity of partner nations in Africa. It also has contributed to disaster response within North America by exploring shelter solutions for the Canadian Arctic and providing aid to first responders in the United States.

Implementing Interactions

Innovation and Scenario Planning for "Wicked Problems." In their classic 1973 treatise, Horst Rittel and Melvin Webber introduced the concept of "wicked" problems to social planning, contrasting "wicked" problems with the relatively "tame" and soluble problems found in mathematics, chess, or puzzle solving.[13] The phrase evokes a

---

[13] Horst Rittel and Melvin Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences*, 1973;4:155–169 [reprinted in N. Cross (ed.), *Developments in Design Methodology* (Chichester: J. Wiley & Sons, 1984),

problem thought to be difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are often hard to recognize. Further, because of complex interdependencies, the effort to solve one aspect of a wicked problem may reveal or create other problems. For DOD, the ability to support the types of contingencies posed by the challenges of globalization, instability, and insecurity from whatever cause is often impeded by limited trust and cooperation with civil-military mission partners,[14] limited abilities to share information and situational awareness, and a lack of suitable, low-cost, support infrastructures. When all three shortfalls are present, the potential for wicked problems is very high.

STAR-TIDES can help the Maritime Strategy address such problems. In complex operations, the United States cannot achieve the social, political, and economic goals for which its military forces have been committed unless it can engage effectively with the populations it is trying to influence. These include local governments, businesses, and members of civil society.[15] These interactions typically involve complex relationships that usually include concurrent mixes of collaboration, competition, and conflict.[16] The ability to share unclassified information is particularly important, as is being able to reach beyond the boundaries of joint military forces and work effectively across other organizational membranes.[17] Unclassified

---

135–44]. The definition of a wicked problem is available online at http://en.wikipedia.org/wiki/Wicked_problem.

[14] Civil-military mission partners include other U.S. Government agencies, international organizations; NGOs; state, local, territorial, and tribal governments; indigenous security services; and others (including commercial firms and individuals as appropriate) who are directly contributing to the ongoing mission. Some NGOs object to the term "partner" and prefer less binding terms like "participant." Private volunteer organizations, largely made up of volunteers, are making increasingly important contributions in complex operations.

[15] See, for example, Mark Gerencser et al., *Megacommunities* (New York: Palgrave MacMillan, 2008).

[16] See "Converging, Combining, Emerging," the Executive Summary of Highlands Forum XXXII, May 29–31, 2007. Available at https://www.hlforum.com/conferences.

[17] See Hans Binnendijk and Patrick Cronin, *Civilian Surge: The Key to Complex Operations—A Preliminary Report* (Washington, DC: National Defense University Press, 2008). See especially chapter 13, "Engaging with Local Actors."

situational awareness and the communications networks to share it are not mere technical adjuncts to combat operations or major HA/DR deliverables such as food, shelter, water, and security. They are the critical enablers of everything else that happens.

STAR-TIDES brings knowledge-sharing and cost-effective infrastructures, but it also includes a planning process that examines scenarios through a structured, multistep approach. The goals of this approach are to *enhance* the ability of civilian coalitions (business, government, and civil society) to operate in stressed environments, *extend* the military's ability to work with civilians in such situations, and *economize* by identifying low-cost logistic solutions and rationalizing supply chains. The scenarios help tie the diverse pieces together.

There is a long tradition of scenario planning within the military, and especially the Navy, as generations of participants in the Naval War College's Global war game may attest. Likewise, the literature of scenario-based planning is wide-ranging and has been shaped by experience in both government and the private sector. Years ago, Pierre Wack wrote in the *Harvard Business Review*:[18]

> Scenarios deal with two worlds; the world of facts and the world of perceptions. They explore for facts but they aim at perceptions inside the heads of decision makers. Their purpose is to gather and transform information of strategic significance into fresh perceptions. This transformation process is not trivial—more often than not it does not happen. When it works, it is a creative experience that generates a heartfelt "Aha" … and leads to strategic insights beyond the mind's reach.

STAR-TIDES emphasizes the needs of affected people "on the ground" who will need to accept, implement, and sustain the solutions. For the purposes of the Maritime Strategy, the global community of STAR-TIDES contributors, plus the "bottom-up" focus, can provide key insights for addressing many of the unique wicked problems inherent in complex, multisector interactions. Moreover, the inclusion of local communities of business, government, and civil society is an important link between strategy and task in support of the cooperative

---

[18] Pierre Wack, "Scenarios: Shooting the Rapids," *Harvard Business Review* 1985(November–December):140. The authors thank Naval Postgraduate School faculty member Marc Ventresca for bringing this article to our attention.

security agenda. These can combine to provide the "Aha" experience mentioned by Pierre Wack.

Some examples provide clarification. The ones below are built around an HA/DR scenario in the Western Pacific.

The first step is for planners, supported by the STAR-TIDES network, to postulate the desired end state and success metrics and to build paths to them from the initial scenario conditions. (How long should people stay in temporary shelters? How will first responders reach the victims?)

Then, drawing on the information in the STAR-TIDES knowledge repository, and especially by "pulsing" the far-flung STAR-TIDES network for ideas, "crosscutting" solution sets can be postulated (mixes of shelter, water, power, etc.) that can be tailored to the needs of the scenario. (Which combinations of shelter, water, power, cooking, etc. would be likely to work best in Western Pacific environments in the rainy season and afterward?) Not all solutions suit all scenarios. Building partner nation capacity to stabilize southern archipelagos calls for different answers (and probably staffing) than supporting mountain earthquake victims in winter.

The most important action is to identify the local, multisector coalition members who will have to live with and sustain the solutions on the ground, and then engage them effectively. (What part of the local government performs FEMA–like functions? What local languages are involved? How do U.S. forces, aid agencies like USAID, the United Nations, and others interact with them?) Social network development and trust building must be combined with bottom-up engagement that focuses on the stressed populations in their environments and also informs top-down project managers. Human interoperability must be encouraged not just among people, but also in institution building and in interactions with available equipment.

The next step is to refine the scenarios, desired end states, metrics, and solution sets in concert with the appropriate local coalition leaders, U.S. entities, and international players. For example, the number of projected homeless may need to be adjusted based on local knowledge, and the postulated infrastructure sets may need to be tailored to local preferences.

Sources of supply need to be identified for the proposed solutions. There are four main options: government stockpiles or contracts, non–U.S. Government stockpiles or contracts, commercial supply chain—indigenous and international, and empowered citizens (if only everyone

had had three days worth of food and water before Hurricane Katrina). As an example of ways to empower civilians, STAR-TIDES is working with computer gamers and the One Laptop Per Child project to write games that could teach children how to prepare themselves and their families better for disasters and how to respond after a disaster hits.

Field operating procedures (including military tactics, techniques and procedures) need to be aligned with policies and doctrine to help people on the ground understand the limits of what can and cannot be shared, what approvals are needed, and so on to work well together. The United States now has fairly comprehensive policy and doctrine about complex operations, but until they are converted into tactical guidance that can be implemented by those in the arena, the results on the ground will be disappointing.

Ideally, these steps will have been taken well in advance of a crisis, and thus form the basis for planning and consequence mitigation.[19] Because information will be widely shared via the STAR-TIDES and related Web sites, others can benefit from lessons learned from any one scenario and apply them to their own situations. Planners in all complex contingencies need to consider what alternatives to traditional command and control[20] need to be designed and implemented for disparate stakeholders in these environments.[21] To let diverse organizations "focus" on problems and develop a shared situational

---

[19] One example is a pending technology demonstration project called PEAK (Pre-positioned Expeditionary Assistance Kits). In conjunction with partner nations, kits will be developed that can support U.S. and partner nations in building the capacity of the partner nations for scenarios of interest to them. These kits will be tailored to local needs and prepositioned in their areas. This work is sponsored by the U.S. Southern Command.

[20] Traditional military command and control typically will not work with civil–military mission partners in complex operations, as nongovernmental organizations, civilian agencies, police forces, and so on usually will not subordinate themselves to military command. This is one reason why it is important to focus on how to achieve unity of effort when there is no unity of command.

[21] David S. Alberts, "Agility, Focus and Convergence, The Future of Command and Control," *The International C2 Journal* 2007;1:1–30. This seminal paper addresses the need, in any contingency, to design structures that focus on the problem, are agile enough to meet the needs of the situation, and can converge the resources to get the job done. NATO is reaching similar conclusions in its reviews of network-enabled capabilities C2 Maturity Models.

awareness of what's going on, network-enabled capabilities are essential that link as many participants as possible. In turn, this requires an underlying data strategy that allows all information on the network to be discoverable, accessible, and understandable. The community of interest for Maritime Domain Awareness is doing this very effectively.

Legal and Regulatory Issues. U.S. Government accountability rules limit DOD's ability to transfer goods and services bought with one kind of funds to other areas under different circumstances. For example, it is hard to leave behind military equipment for disaster victims. Both the Maritime Strategy and STAR-TIDES need to understand these constraints and address them as appropriate. In addition to general rules on equipment transfer, planners must understand what regulatory and other issues must be addressed in particular scenarios (customs and border clearance, or export controls, for example).

The distributed nature of modern information sharing raises an important question that will have to be answered by governments and other organizations in the next few years. That involves the oversight of and accountability in so-called covenantal arrangements. There are well-established procedures for managing accountability and oversight in command relationships and in contractual relationships, but there are few models for inspectors general and accountability offices to use when the arrangements are made by covenant (e.g., handshakes, distributed data storage outside a firewall like Google Docs, agreements among disparate cultures—"three cups of tea," etc.). [22] Many activities in complex civil–military operations, Web 2.0 environments, and other situations in which there is no unity of command will have to rely on covenants. This is an important issue that will have to be addressed from many standpoints—managerial, policy, legal, and accounting. Both the Maritime Strategy and STAR-TIDES efforts to promote partnerships among diverse organizations will have to engage here as well.

Training, Exercising, and Education. A key part of any program is to train the trainers first, and then those who will use the infrastructures in the field. Rotary Clubs do an excellent job of this in

---

[22] The authors are indebted to Mr. Ken Hamilton of the KENTIA Management Group for this insight.

supporting deployments of the ShelterBox disaster relief kit.[23] ShelterBox will deploy a team of trainers who speak the local language to teach local Rotarians how to set up the tents and use the shelter box equipment, so that they in turn can train survivors. Exercise programs are needed to practice, refine, and revisit issues; incorporate lessons learned; and change behaviors. Some broadly inclusive exercises can be used as models, including Operation Golden Phoenix, which involved more than 140 different partners in the summer of 2008, and the annual FA-Hum (*Fuerzas Aliadas Humanitarias*) disaster management event sponsored by SOUTHCOM, which engages more than twenty Central American and Caribbean nations, U.S. military forces, and transnational institutions.

Transformational Aspects of STAR-TIDES and the Maritime Strategy

As noted earlier, transformation involves changes in people, processes, organizations, and technology. Both the Maritime Strategy and STAR-TIDES invoke crosscutting changes among all of these areas. A good expression of how these linkages can work is expressed in the book *Democratizing Innovation* by Eric von Hippel, professor and head of the Innovation and Entrepreneurship Group at the MIT Sloan School of Management, in Boston, Massachusetts. The book describes how people participate in the development of products they use and explains in detail the emerging process of user-centric democratized innovation. Von Hippel states:[24]

> It is now clear that users often innovate, and that they often freely reveal their innovations. But what about informal cooperation among users? What about organized cooperation in development of innovations and other matters? The answer is that both flourish

---

[23] http://www.shelterbox.org/home.htm. The ShelterBox Trust is a registered U.K. charity that provides emergency aid for victims of natural and other disasters anywhere in the world. Since operations began in January 2001, it has helped over 800,000 people and worked in more than 52 countries, responding to earthquakes, floods, hurricanes, tsunamis, wars, volcanoes, and so on.

[24] Eric von Hippel, *Democratizing Innovation* (Cambridge, MA: MIT Press, 2005), 93. The book is also licensed under a Creative Commons license and is available as a downloadable PDF document on http://web.mit.edu/ evhippel/www/democ.htm.

among user-innovators. Informal user-to-user cooperation, such as assisting others to innovate, is common. Organized cooperation in which users interact within communities, is also common. Innovation communities are often stocked with useful tools and infrastructure that increase the speed and effectiveness with which users can develop and test and diffuse their innovations.

As illustrated in the scenario analysis example, the STAR-TIDES innovation community can address planning issues quickly, at several levels, in ways that can improve the abilities of the Sea Services and regional combatant commanders to engage complex operational challenges. This is especially true when the interactive tools of social software and Web 2.0 are brought to bear.[25] Moreover, diverse groups can explore multiple dimensions of the interactions among people, processes, organization, and technology to promote innovative, crosscutting interactions in a number of ways. Six examples follow.

People and Processes. The Maritime Strategy and STAR-TIDES both focus on preparing people for new types of missions in complex, networked environments. Both promote more integrated processes among governments, nongovernmental organizations, international organizations, indigenous entities, and others in support of "relevant populations." An important part of this is to convert strategy, policy, and doctrine into effective field operating procedures quickly. In addition to learning how to write such procedures, the Sea Services should pursue human interoperability and organizational research to develop trust and build social networks before they are needed in crises.

People and Organizations. A common theme of the Maritime Strategy and STAR-TIDES, as well as the work of the Transformation Chairs network, is that education is a very important, even strategic, investment for the United States. This is less traditional education than the conversion of educational approaches to promote innovative, adaptive thinking, and lifelong learning. In parallel, U.S. national security institutions, including the Sea Services, need to change their cultures to emphasize experience with complex operations when selecting people for leadership positions and promoting them. This

---

[25] See, for example, Mark Drapeau and Linton Wells II, "Social Software and National Security, a 'Net Assessment,'" Defense and Technology Paper 61 (Washington, DC: National Defense University, Center for Technology and National Security Policy, 2009).

typically requires that lessons from real-world activities be learned and converted quickly into changed organizational and individual behavior.

People and Technology. Technological solutions for complex operations must be affordable, implementable, and sustainable by indigenous, "relevant populations" in their worlds—not just by U.S. or coalition forces or aid organizations. Initiatives such as the Global Maritime Partnership recognize this as they work to engage the world's navies and coast guards, often in their waters, and help develop their capabilities. In the same vein, STAR-TIDES expressly looks for alternatives to expensive DOD programs of record in favor of those more suited to building partner capacity. In both cases, Sea Service personnel can benefit by thinking more broadly about how crosscutting, "whole systems" approaches (using different systems together) can increase effectiveness by integrating disparate technologies.

Processes and Technology. Unclassified information sharing with civil–military mission partners beyond the boundaries of the Joint Force is essential to success in the kinds of operations addressed by both the Maritime Strategy and STAR-TIDES. This often involves relatively low-tech solutions, including collaboration tools that can work with users who have limited access to communications. This requires changes in traditional military communications processes that emphasize links within the boundaries of joint forces, rather than beyond them. In support of such shifts, the April 2009 DOD instruction on unclassified information sharing[26] and the provision of Internet access to nongovernmental organizations on Maritime Partner station ships[27] are important steps forward.

Processes and Organizations. In recognition of the growing importance of complex operations, civilian deputies have been established for the four-star commanders of both the U.S. Southern and Africa Commands. This truly reflects transformational organizational change. The growing use of covenantal relationships, discussed earlier, will require significant shifts in organizational processes to achieve a balance between decentralized innovation and oversight with accountability. Finally, the Sea Services and the STAR-TIDES research

---

[26] DODI 8220.02, "Information and Communications Technology, Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations," April 30, 2009.

[27] Naval Studies Board, *Maritime Security Partnerships* (Washington, DC: National Academies Press, 2008).

network should work together, along with the Center for Complex Operations (CCO) and others, to help partner organizations implement lessons learned and adjust educational curricula accordingly.[28] Profoundly innovational outcomes can result.

Technology and Organizations. Information technology enables the flat, porous network of STAR-TIDES, as well as the data-based communities of interest that are essential for accurate maritime domain awareness. In turn, such awareness demands expanded intelligence, surveillance, and reconnaissance, as well as interagency (and international) information-sharing and cooperation. This is true not only for combat operations, counterterrorism, antipiracy, and counternarcotics but also for humanitarian assistance/disaster relief. The ability to gain situational awareness rapidly and share it widely is the critical enabler of all other actions in these situations. What is transformational is that this can be achieved with relatively low-cost systems and distributed, federated organizations, based on responsible sharing and collaboration.

Summary

The Maritime Strategy calls for persistent engagement at all levels to build enduring relationships and promote understanding with nontraditional partners to help avoid conflict. STAR-TIDES' multidisciplinary, international approaches and linking of distributed talent already are contributing solutions to real-world challenges. Both include transformational elements that cut across people, processes, organizations, and technology to facilitate public–private, whole-of-government engagement to improve performance in complex environments. These complementary efforts can help build global partnerships to address the challenges of globalization, instability, and insecurity in the 21st century.

---

[28] The Center for Complex Operations is a developing "community of practice" of civilian and military complex operations training and education institutions and practitioners (see essay 4). The CCO defines complex operations as consisting of counterinsurgency; stability, security, transition, and reconstruction operations; and irregular warfare. The authors have adopted a more expansive definition that includes humanitarian assistance and disaster relief at home and abroad.

Essay 6

WikiForce

Global Cooperation in New Security Structures

By Henrik Friman

Abstract

In 2005, Admiral Mike Mullen, U.S. Chief of Naval Operations, proposed the Global Maritime Partnership (GMP). His concept was to create a 1,000-ship Navy consisting of 313 American military ships and approximately 700 ships from trusted partners, including Sweden. The United States will provide ships able to operate on the open sea, and the partners will predominantly contribute ships adapted to the geographical areas where the GMP will operate. This 1,000-ship Navy may be the first example of a WikiForce, that is, a developed, adaptive way of organizing for the future.

Usually discussed in the context of business and academia, wikis are technical solutions that enable cooperation by simplifying publication and updating of information through open, Internet-based technology. The best-known example of a wiki is Wikipedia, an online encyclopaedia that contains millions of entries compiled and maintained by innumerable contributors working independently. Other examples are: MySpace, Flickr, Second Life, YouTube, Linux etc. Tapscott (2006) describes how the business community has made use of wiki technology and how the new technologies created what he calls Wikinomics. Wikinomics is based on mass communication and contains tools that enable openness, connectivity, and sharing and facilitate acting globally. Applying logic similar to that described by Tapscott in Wikinomics, new defence concepts are now possible, such as the 1,000-ship Navy—a WikiForce.

A WikiForce has not previously been discussed conceptually. In this text an introductory description is made of how WikiForces can organize professional forces and how these principles can support the construction of future security structures. As its starting point, the discussion brings insights from wiki society, from the perspective of military development.

103

Introduction

In the literature, there are comprehensive descriptions of how the Information Age's various technical innovations have come to influence military security structures. This development is known in everyday language as Force Transformation, which can be summarized with the words digitalization and globalization (Friman and Higgins, 2007). The digitalization of society, for instance, in the military security sector has influenced preconditions in a number of areas. Nowadays, military operations have sensors that are able to collect high-quality data—almost in real time—that quickly can be processed to situation maps that are disseminated globally to a large number of users, almost regardless of where those who need information are. As a preparation for coming efforts with new technology, events can be modulated and simulated ahead of time. Technology can be produced as extremely small units and tailored solutions through so-called nanotechnology, thereby reducing costs for transports and possibility for discovery, while at the same time increasing life span and efficiency. There are technological advances underway in a number of areas that directly affect the military security area, which in turn creates new conditions for how military operations can be carried out and accelerates demands for new ways of working and organizational structures.

At the same time as the information age's technological advances are making an increasingly clear entry into society, there has been a change in the military challenges. Since 9/11 and the tsunami disaster, which can be described as shocks for security planning, increasingly high demands are today being made on military units to be able to contribute in situations that traditionally have been regarded as civilian rescue operations. Military units are today given an increasingly clearer role in crisis situations, and the need to be able to interact multinationally and with nontraditional players—for instance, other authorities, companies, and relevant organizations—increases.

The military profession was previously seen as a resource to be deployed when society's other resources was not adequate. At this time, however, defense is increasingly being given tasks in the forefront of the rescue services. The military is no longer the "strategic reserve" of the rescue services' leader but can be seen as an active component to be deployed at an early stage to solve situations that have

arisen, which demands that the military profession also must include what were previously seen as civilian competencies.

The transformation of the military has entailed that today's defense forces have been given increasingly global tasks, in which, for example, Swedish units at short notice can be deployed far beyond Swedish territory in internationally assembled units. The Swedish defense has made the transition from a mobilizing defense to a mission-oriented defense. The development in society and the defense mean that new security structures are being developed. The innovation force that has driven developments in the area of technology spills over to innovative organizational solutions. These new organizational structures take increased consideration of global security thinking for solving tasks that are conceivable for the future.

The condition for military organizations to be able to function in the situation described here is heavily dependent on how the organization can be coordinated and can interact with other players. The capacity for cooperation should be considered one of the most decisive factors for success in future crises or wars (Bordetsky & Friman, 2006). Today this conclusion is shared by relatively many people, and there is currently a large amount of work underway for the development of a climate for cooperation within the field of the military profession. In the debate there is talk of the wiki society. The question raised in this text is, how the wiki society's insights and challenges are conceptually thought to be designed for military operations with regard to profession, organization, and security.

The Wiki Society

For most people the Information Age has come to be associated with the Internet and with sending digital messages via e-mail, SMS, and MMS instead of handling paper with faxes and written letters. Within the business world, among other areas, so-called wikis are being discussed and introduced as an active component in everyday work. Wikis are technical solutions that enable cooperation by simplifying publication and updating of information via Internet-based technology. The best-known wiki application is Wikipedia, an online encyclopedia that contains millions of entries contributed and constantly refined and updated by innumerable users who need only minimal knowledge of how to use a computer. Wikipedia is an international knowledge bank that is continuously growing and evolving. Earlier encyclopedias, such

as the National Encyclopaedia and Encyclopaedia Britannica, took decades to produce and offered limited opportunities to be supplemented, updated, or corrected after publication via supplementary sheets and volumes. Those paper encyclopedias could be searched only by persons with physical access to them. Wikipedia can be searched by anyone with access to a computer—including handheld devices—and an Internet connection.

Examples of technologies that facilitate universal information sharing and social networking—collectively called social media—include Twitter for brief text communications among subscribers, MySpace and Facebook for personal publication of an individual's own data; Flickr for sharing of images and video; Second Life for interaction via avatars in a virtual world; YouTube for publication of video clips; and Linux, an openly developed operating system for personal computers. These technologies have in common that they are developed in cooperatively by users of the services.[1]

What distinguishes the wiki society from the previous information society is the level of collaboration enabled by new forms of connections. Early on in the information society, the focus was on how to make information available for as many users as possible; in today's wiki society, it is more about how to be able to cooperate with as many people as possible, thereby increasing productivity and effectiveness. It should be apparent that this altered focus on availability of information has professional and organizational consequences. Whereas earlier organizations focused on producing and spreading messages through information by emphasizing "credible" places/sites, today the focus is on a credible collaboration partner with clear relations to other credible partners. Confidence is the key to common projects such as wikis.

An author with a particular interest in the development and implications of the information society is Don Tapscott, who described in 1993, together with Art Caston, a paradigm shift in business based on the development of information technology. They argued that information technology would significantly change the business life of the future in a more open and client-oriented way.[2] In 1998, Tapscott published *Growing Up Digital: Rise of the Net Generation,* which was

---

[1] For a more extensive description of social media see Drapeau & Wells (2009) and Crebolder et al. (2009).

[2] Don Tapscott and Art Caston, *Paradigm Shift* (New York: McGraw-Hill, 1993).

about the profession of the coming "net generation." The book discusses how new kinds of organizations through so-called communities and workspaces, affect the way people meet and exchange information, and where issues of loyalty and belonging are highlighted,[3] together with nationalism. These are many of the thoughts and ideas that can be seen today within the development of tools for collaboration, for which wikis have been used as illustrative examples in this text.

Two years later, Tapscott, together with David Ticoll and Alex Lowy, published texts about digital capital that were about how to do business on the Web.[4] In the book, the first steps were taken toward his book *Wikinomics*. The arguments behind digital economics are still colored by the economic models that prevailed in the industrial society and early information society. It was not until *Wikinomics* that the step with wikis was fully taken. *Wikinomics* is based on mass communication with tools that facilitate openness, connectivity, and sharing and that enable global action.[5]

By following Tapscott's work over the last 15 years, an image of the development of the information society is created in which previous logic, structures, and regulations are strongly questioned. It is no longer reasonable to believe that the new information technology only could lead to automatization of previously known processes. Completely new kinds of attitudes and behavior have been created, which in turn leads to new kinds of operations. A similar development is underway today in the military area. Previously tightly bound national defense structures are now being dismantled and reshaped as parts of international security structures that can be used far from the national territory. It is, in this context, exciting to study Admiral Mike Mullen's launch of the concept of a 1,000-ship navy. Could it be that the U.S. Navy has adopted the logic of the wiki society, and that the time is now ripe to create what could be called a WikiForce?

---

[3] Don Tapscott, *Growing Up Digital: Rise of the Net Generation* (New York: McGraw-Hill, 1998).

[4] Don Tapscott et al., *Digital Capital: Harnessing the Power of Business Webs* (Boston, MA: Harvard Business School, 2000).

[5] Don Tapscott and Anthony D. Williams, *Wikinomics: How Mass Collaboration Changes Everything* (New York: Portfolio, 2007).

The Wiki Force

Cass Sunstein (2006) described a conceivable future American Department of Defense based on a wiki system in which manuals and regulations are written as wikis. Examples that are taken up are WikiLaws, in which critical legal issues are dealt with, and how higher civil servants are updated and inform each other about the development of events in various regions through shared and jointly built information surfaces.[6] Sunstein's forward thoughts are today a reality. On June 2, 2009, the U.S. Forces–Afghanistan command launched a Facebook page, Twitter feed, and YouTube page to communicate the Afghan mission to the world via cyberspace. Since beta testing began on May 12, 2009, the U.S. Forces–Afghanistan Facebook page has drawn more than 4,700 fans, and more than 1,400 people and organizations have signed up to follow its tweets on Twitter. There was no active marketing of either site during the beta testing period.[7] The number of portals and blogs in the military domain is increasing rapidly, and common texts are being developed with the help of new technologies. The development has progressed so far that Dave Wennergren, Deputy Assistant Secretary of Defense for Information Management and Technology and Deputy Chief Information Officer, stated at the conference WEST'07 that no more portals are needed. The information supply through digital information surfaces is on such a massive scale that what is now in demand is surfaces that increase the value of available information.

In 2005, Admiral Mike Mullen, then-U.S. chief of Navy Operation, proposed the Global Maritime Partnership concept, creation of a 1,000-ship navy consisting of 313 American ships, plus approximately 700 ships from other trusted partners. Not even a great power like the United States is today able to organize and equip a naval force that can manage every challenge of the future security situation. The world economy is today interconnected, and regional crises can rapidly lead to global consequences. The many environments and diversity of threats requires flexibility and presence in many areas, and the U.S. Navy has today made the transition from having land-based base areas to being largely sea-based. To manage the increasingly comprehensive commitments to global security, a dialogue is now being initiated with

---

[6] Cass R. Sunstein, *Infotopia: How Many Minds Produce Knowledge* (New York: Oxford University Press, 2006)

[7] U.S. Forces–Afghanistan, press release 20090206-01, June 2, 2009.

"allied" partners to manage future challenges together. In this context, Sweden has been asked to participate in the development of the 1,000-ship navy and has responded positively.

The idea is to create the capacity for global maritime security through cooperation, in which national navies will function as global ambassadors.[8] The United States has taken on the role of providing ships that are able to operate on the open sea, and the remaining nations will contribute with ships that are more specifically adapted for the geographical area in which Global Maritime Partnership will operate. An example of this is drug control and piracy operations in U.S. Southern Command (SOUTHCOM): "SOUTHCOM strives to halt the flow of illegal drugs into the United States by supporting the region's multinational effort to combat narcoterrorism, threats to legitimate governments, and dangers that are the direct result of the production and sale of those drugs. SOUTHCOM missions to combat this threat are twofold. Counter Drug operations involve the detection, monitoring, tracking and interdiction of drug runners. Counter Narcoterrorism operations are those where U.S. military forces provide support to partner nations that are combating narcoterrorist groups within their borders,"[9]

At first glance, the concept may be experienced as a new way of organizing international marine battle forces, but with more in-depth analysis, one discovers that the 1,000-ship navy may be the first example of a WikiForce, that is, an entirely new way of organizing for the future. The 1,000-ship navy goes beyond sharing information surfaces to actually sharing resources and tasks.

The U.S. Office of Force Transformation had previously initiated a study of the development of future maritime battle forces, Task Force 50.[10] Task Force 50 was a maritime battle unit active during Operation *Enduring Freedom*, the commander of which developed a command system based on wiki technology.

> We wanted a better method for distributing information across the battle group. We didn't want it to make the war fighter's job harder. Rather, we wanted to prevent duplication of effort. We needed a dynamic warehouse of continuously updated information. Above all,

---

[8] U.S. Navy PowerPoint presentation, 1,000-ship Navy, November 2006.
[9] http://www.southcom.mil/AppsSC/pages/counterNarco.php
[10] http://www.oft.osd.mil/initiatives/ncw/docs/TF-50%20HBR%20_Final_pdf.

it had to filter and format information, eliminating the spam, adding value to the information, and ultimately improving speed of command.

—Rear Admiral Thomas E. Zelibor

The result was that the battle group changed its behavior, from having staff meetings for sharing of information to devoting more time to solutions of the operation. In the final report, one can read:[11]

Evidence gathered in this study suggests that it takes not only sophisticated technology and money to facilitate transformation. It also requires the synergistic development of technology and funding, as well as the co-evolution of organization, people, process, trust, and of course, strong leadership and an environment that will allow transformational people to initiate and sustain innovation.

The Wiki Organization

On a number of occasions, arguments have been put forward that the use of the wiki concept changes attitudes and behavior, as well as the way activities are organized. Despite this, relatively few new organizational forms have been presented in the literature. The argument can be seen as traditional and is primarily about switching from centrally governed and regulated planning and control routines to decentralized and more self-organized organizational forms. Initiatives such as Wikipedia challenged traditional encyclopedias not only in their functionality but also in the way in which development happens and is governed. The power and control of the development is no longer in individual institutional organizations but has shifted to the users. This trend shift has been described by Alberts and Hayes as edge organization.[12]

Edge organization is a structure that is predicted to be more agile than traditional structures. It is a structure in which allocation of decision mandates, increased interaction, and increased distribution of information create better conditions for functioning.[13] In one of the

---

[11] Office of Force Transformation, "Task Force 50 During Operation ENDURING FREEDOM," U.S. Office of Force Transformation (2006), 22.

[12] David Alberts and Richard Hayes, *Power to the Edge: Command Control in the Information Age* (Washington, DC: CCRP Publication Series, 2003).

[13] NATO RTO, SAS-050 study group, panel's final report. Available at http://www.dodccrp.org/files/SAS-050%20Final%20Report.pdf.

North Atlantic Treaty Organization's work panels[14] work is underway in developing the future concept of command and control. Today the direction is to see command and control based on five stages of organizational development (contradictory, neutral, coordinated, interacting, and mutual) that are better at describing the future than today's command and control models. Table 1 is a compilation of the factors that have been deemed to be of particular interest for describing the five stages of development.

We know from earlier research that the organizational structure is affected by the set task, as well as the conditions under which the organization is expected to function. This means that if the work is conducted in stable and relatively predictable situations, organizational forms that can be expected to exist during the lower stages of development can handle the situation very well. However, if the circumstances become volatile and unpredictable, increasingly higher stages of development must be used. It is plausible that the relationship between different players in a particular field will change over time and that there are different stages of development for different players.

Of particular interest is how transfers between the various stages of development occur, rather than identifying at what level the organization is. Even if the latter aspect may be considered important for creating an understanding of the actual working conditions, it is by being better able to understand the dynamics of the development from, for example, neutral to coordinated or coordinated to interacting that improvement is accomplished. With greater understanding, the commanders are given instruments and indicators of how the organization's functionality should be developed to best complete set tasks.

---

[14] NATO RTO, SAS-050 study group.

	Contradictory	Neutral	Coordinated	Interacting	Mutual
Allocation of decision mandates	None	Accept restrictions of decision rights	Accept dependencies	Delegated decision mandate and acceptance of internal dependencies	Dynamic allocation of decision mandates
Interaction	None/antagonistic	Communicate restrictions	Interaction on coordination factors	Ongoing cooperation Dynamic feedback	Adapted to situation United
Information distribution	None	Distribution regarding restrictions	Rich information about dependence relationships	Continuous information flows	Smart push
Other factors	None	Accept restrictions	Limited shared effects Coordination plans	Confidence Create Coordination mechanisms Interaction plans Synergies	Self-synchronized Edge organization Shared control

Table 1. Stages of development based on Edge organization criteria. (Part of data and underlying information from NATO RTO SAS-065 working group)

112

Contradictory–Neutral	Neutral–Coordinated	Coordinated –Interacting	Interacting–Mutual
Identify dependencies Establish dependencies Create dependencies (links)	Partly shared objectives Selected coordinated functions Coordination mechanisms	Ongoing acceptance of shared risk Shared understanding Developed confidence Shared intention Interaction plans Interaction mechanisms	Stable shared intentions Stable shared awareness Stable shared understanding Increasing self-awareness across system boundaries

Table 2: Transitional Factors between Different Developmental Stages (Source: Part of data and underlying information from NATO RTO SAS-065 working group)

To manage the transition from an interacting to a mutual organization, new thoughts and ideas for command and control and structuring are required. Traditional organizational structures that are based on Barnard's (1938) ideas about organizations—that when persons are prepared to contribute to the operations they can communicate with one another to achieve common objectives—can partly be questioned.[1] At the mutual level, the operations occur based on organizational borders, and the question of how self-awareness is affected across system boundaries becomes of increasing interest. The question regarding which organization one belongs to becomes increasingly subordinate to the question of understanding intentions and creating opportunities to meet imminent challenges. By creating more innovative organizational forms, flexible structures adapted to the situation are developed that can be changed dynamically as the development of events is underway. At the same time, traditional and ingrained roles and patterns are challenged. Commanders, who previously had been given clear areas of responsibility and resources, are placed in a new situation, facing increased insecurity, where they

---

[1] Chester I. Barnard, *The Functions of the Executive* (Cambridge, MA: Harvard University Press, 1938).

are no longer given clear mandates in the traditional meaning. Moral and ethical standpoints concerning right or wrong are more prevalent now, even at lower organizational levels.

The reasoning is based on every organization having a number of relationships to different partners. In certain relationships, the organization can have contradictory relationships at the same time as the relationship to others can be interacting or mutual. With this as a starting point, the organization becomes a kind of positioning in relation to other units over time. For the higher forms of cooperation to function, there must be loyalty and trust. Without loyalty and trust, the conditions for wanting to cooperate and take risks will be lacking.

The issues that can be seen in the different developmental levels can be described on a scale from function- to process-oriented. This means that in contradictory relationships, it is primarily functions that develop in isolation and in competition with one another. In neutral situations, dependence in function and process are established, whereas in the coordinated stage, the focus is more on processes to create functions. At the interacting level, it is primarily processes that are jointly handled to mutually provide opportunities for testing entirely new forms, described in this text as innovative organizational forms.

Contradictory	Neutral	Coordinated	Interacting	Mutual
Function-oriented	Function- and process-oriented	Process- and function-oriented	Process-oriented	Innovative organizational forms (Edge Organization)

Table 3: Developmental Stages

Innovative organization forms have a stable and conscious sharing of intentions under increasing self-awareness across system boundaries. There are striking similarities with the previously described WikiForce. Both the same logic and course of action for achieving results can be found in the mutual level, as in WikiForce. Under these conditions, the demands on the military profession will also change.

Wiki's Demands on the Profession

With the change described here as a starting point, the question can now be raised as to how the profession—military commanders—will be

affected if a WikiForce becomes reality. It is too early to be able to give a clear-cut answer today, but a number of interesting observations can be noted.

The military profession has traditionally been likened to an administrative profession. Military commanders are expected to command and control operations. The ability to develop plans, optimize resource allocation, and perform ongoing follow up has been rewarded. The operations are then assumed to function within a given framework and own responsibility known as task tactics. In reality, only limited freedom to act is given because the framework completely governs the operations. Based on the principles of a WikiForce, the profession will be more about creating conditions for solutions in which several interacting parties are involved. A future military commander's potential to succeed lies in their ability to influence the interest of these interacting partners to achieve desired results, rather than in perfecting plans. In contrast to the administrative schools of leadership, I believe that the development of the profession is moving from governance and control to interaction design and an understanding of the possibilities of exerting influence. Commanders will search for real options in their problem space and will be judged on their ability to recognize opportunities.

Future military commanders have traits that are in many ways similar to the way entrepreneurs are described in the literature. Based on Burch's (1986) description of entrepreneurs,[2] table 4 provides a hypothetical list of characteristics of military commanders in innovative organizations.

The development of the military profession is influenced by previously well-designed and well-trained units to specific tasks that are deployed in relatively known environments. Today network units are being developed that are constantly in a design stage without clear tasks. The challenge for these units is to create routines and structures while at the same time trying to avoid blockings that make the unit less flexible. It is the task of the military profession to balance the unit's rationality through coordinated efforts, while at the same time retaining flexibility.

---

[2] John G. Burch, "Profiling the Entrepreneur," *Business Horizons*, 1986;September–October:13–17.

Conclusion

WikiForce is a concept of great importance in which small countries such as Sweden, together with larger players, can create security structures that would otherwise not be possible. For instance, within the Swedish–Norwegian cooperation that is now underway, there are far-reaching plans for mutually shared functions. The cooperation between national armed forces is becoming increasingly tangible and real. Many say that this is a sign of globalization, but without value being added in the process, no investments will happen. There is today a tangible value added by cooperating across national borders.

We must not underestimate the technical challenges in creating a WikiForce. One of the main challenges is the security of our systems. It is not satisfactory, as in today's wiki system, to build a national security solution on the principle that it is self-correcting. Without more research on creating secure systems we cannot trust to a WikiForce to function. Wiki systems are now part of our daily operations, and we must now work to take advantage of them when we build national security.

The WikiForce concept creates greater dependence on other parties. By going down this path, Sweden creates dependence on allied partners and forfeits the ability to remain neutral. Sweden has a long tradition of a "total defense" concept, meaning that the country had all resources needed for defending the nation, even if it had little of these resources. The transformation will shift the focus from total defense to selective capabilities that could be included in a collaborative force. If these capabilities are of no interest to other parties, will Sweden be welcome in a collaborative force?

Desire to achieve	A pressure to overcome problems, and create conditions for successful initiatives
Hardworking	Works far beyond regular work hours to manage to keep all relations "alive"
Desire to work in proximity of others[3]	Works well together with other individuals to generate desired knowledge and results together This trait requires a good ability to negotiate and look for so-called win–win situations to be able to establish mutual trust
Nurtures quality	The will to take responsibility and monitor initiatives until they are self-regulating
Accepts responsibility	Is morally, legally, and mentally responsible for initiatives; there is a focus on own benefits
Reward-oriented	Aims at succeeding, works hard, and takes responsibility, while at the same time desiring appreciation and compensation for their efforts. This can be values other than money, such as appreciation and respect
Optimism	Lives according to the philosophy that this is the best of times and that everything is possible
Oriented toward excellence	Frequently aims at creating exceptional results that they can be proud of

Table 4: Hypothetical Traits of Future Military Commanders

---

[3] This trait contrasts with Burch's view, whereby Burch spoke of the entrepreneur as a person who preferably works alone, which is not compatible with increased mutual interaction.

References

Alberts, D. & Hayes, R. (2003). *Power to the Edge: Command Control in the Information Age*. Washington, DC: CCRP Publication Series.

Barnard, C.I. (1938). *The Functions of the Executive* (Cambridge, MA: Harvard University Press).

Burch, John G. (1986). "Profiling the Entrepreneur," *Business Horizons*, September–October, 13–17.

Crebolder, J. et al. (2009). "Investigating Virtual Social Networking in the Military Domain," Proceedings of the 14th International Command and Control Research and Technology Symposium, Washington, DC, June 15–17.

Drapeau M. & Wells II, L. (2009). "Social Software and National Security: An Initial Net Assessment," *Defense & Technology Paper 61*, Washington, DC: National Defense University, April.

Mintzberg, H. (1983). *Structure in Fives: Designing Effective Organizations*. London: Prentice-Hall International, Inc, 143ff.

Sunstein, C.R. (2006). *Infotopia: How Many Minds Produce Knowledge*. Oxford: Oxford University Press.

Tapscott, D. & Caston, A. (1993). *Paradigm Shift*. New York: McGraw-Hill.

Tapscott, D. (1998). *Growing Up Digital: Rise of the Net Generation*. New York: McGraw-Hill Inc.

Tapscott, D. et al. (2000). *Digital Capital: Harnessing the Power of Business Webs*. Boston, MA: Harvard Business School Publishing.

Tapscott, D. & Williams, A.D. (2007). *Wikinomics: How Mass Collaboration Changes Everything*. Portfolio.

U.S. Navy. "1000 ship navy," PowerPoint presentation, November 2006.

U.S. Office of Force Transformation. (2006). *Task Force 50 During Operation ENDURING FREEDOM*, U.S. Office of Force Transformation.

Essay 7

Emergent Leadership

Linking Complexity, Cognitive Processes, Adaptability, and Innovation

By Sandra Martínez

Abstract

A paradigm shift in our understanding and practice of leadership is required to meet 21st-century national security challenges. The author argues that emergent principles and processes observed in complex natural and social systems offer valuable insight, a framework for inquiry, and a blueprint for change. The author explores the phenomenon and mechanisms by which emergence of novel structures and processes arise in systems operating at the "edge of chaos" and discusses the opportunities and constraints of self-organization, linking social science literature to literature on command and control generated by the Department of Defense. Then the author presents a conceptual framework for leadership development and "systemic interventions" to support transformation. The Leadership Development Framework is compatible with a view of leadership that is emergent, collaborative as well as competitive, and complex, and captures the dynamic outcomes of interdependencies among many agents. A description of the pilot action research project conducted in 2008 at the U.S. Army War College on complexity leadership and development, supported by the Transformation Chairs, follows. The author concludes with recommendations for the education and development of national security professionals based on the results of the study and emergent principles.

Introduction

Advances in information and communications technology enable continual interaction among individuals, teams, networked groups, organizations, and societies. In this way, technology has accelerated the process of globalization, the process whereby ideas, labor, capital, and goods cross national borders with few barriers. This

dynamic exchange has qualitatively changed the environment by making it more complex. Globalization has created interdependencies among and between nation-states, markets, non-state actors, and other constituent parts of our social, biological, and physical ecosystems. Contrary to initial predictions, the process of globalization has not brought about a convergence of culture but, rather, reflexivity about one's own culture and identity in relation to others (Guillén, 2001). Information technology has rendered knowledge accessible along the critical dimensions of time and cost, with both positive and negative outcomes. The churn of ideas and practices made possible by this interconnectedness presents great opportunities for innovation and creation of wealth. However, it has also introduced the challenge to national security of asymmetric conflict with unofficial actors or rogue states that leverage the power of a networked organization using these technologies. It has also wrought the reality of 24/7 media and communication, which has increased the strategic significance of information warfare. In summary, the dynamic complexity of the environment, intensified by the advances in information and communication technology and other new technologies, has changed the "metabolic rate" of knowledge processing and creation and the rules of the game, and thus the dynamics of power.

It is clear from the 2008–2009 financial crisis that we have not fully considered the effects of these interrelationships, nor do we understand the rules governing these interdependent complex systems in which natural and human systems collide. Yet, the challenges of natural security in such an environment require us to strive to understand the logic, underlying structures, patterns, and mechanisms of the interrelated systems within which we live and to which we contribute so we can use this knowledge to act effectively.

This essay argues that a new way of understanding the world, a shift in paradigm, is required to successfully negotiate constructive action in this environment. This shift involves drawing from the advances in our understanding of dynamic complex systems—knowledge originally developed in the natural sciences of physics, chemistry, and biology that for the last 15 years has influenced the social sciences. Drawing from the body of knowledge based on emergent principles or complexity science to understand social systems in the context of national security issues, in particular, has a history and numerous precedents. After World War II, the mathematician John van Neumann explored self-replication in machines in his work with cellular

automata—abstract robots represented as cells on the computer screen operating under a set of rules. This research was partly motivated by the problem of the reliability of U.S. Air Force missiles (Goldstine, 1972). Vice Admiral Cebrowski and John Garstka (1998), in their development of the concepts of network-centric warfare, also drew from this scientific foundation. The U.S. Department of Defense Capstone Concepts for Joint Operations of 2005 described the organization of the Department of Defense, its adversaries, and the environment as complex adaptive systems. In addition, the United States Army *Commander's Appreciation and Campaign Design* (2008) incorporates the concepts of complex adaptive systems; discusses nonlinearity; recommends approaching problems in a more holistic and less reductive manner; emphasizes the importance of reflection, learning, and adaptation; and quotes John Holland (1995), who was one of the key theorists in the development of emergent phenomenon, to describe distributed, noncentralized "direction." However, a paradigmatic shift, as we know from the work of Kuhn (1962), involves a fundamental change in the set of assumptions that undergirds a causal explanation of the world. This transformation in thinking and practice has not occurred within U.S. national security institutions. A better understanding of the mechanisms supporting emergence and self-organization and the role of leaders in shaping and influencing direction and outcomes within organizations and interorganizational initiatives is necessary.

Paradoxically, although the great power of computers allows us to explore and gain insight into the self-organizing process of physical, biological, and social systems, which are often accessible on our own computer screens, we concurrently are confronted with the limits of our knowledge. We realize that we can never know and understand complex systems completely and that these systems are creative and ever-changing, and do not easily yield to prediction or control. The emergence of order spontaneously from the interaction of agents loosens the deterministic, linear connection between a particular action or cause and the ensuing outcome challenging our conventional rationalist paradigm. Richardson (2008) emphasizes the incompressibility of our knowledge of systems—that we cannot represent a system accurately in anything less than a representation of the whole system because whatever we omit may have nonlinear, and thus unpredictable and disproportionately large, effects. Nonetheless, we can move forward with the knowledge that we possess to enlighten

particular aspects of a system. Ironically, as the scale of our exploration in time and space enlarges, we begin to recognize the limits of our understanding. Some humility and even reverence in the face of this creativity, recognizing our place in the universe, may be an important aspect of this paradigmatic shift (Kaufmann, 1995).

Although there are many critical processes of national security, including strategic planning, that would benefit from a deeper understanding of emergent principles, it is perhaps in the domain of command and control principles, processes, and practice where its effect is most overarching, for several reasons. First, the principles of centralized command and control, although they have been slowly changing for centuries, are core values of the military—often unexamined principles emphasized in military training and education (Alberts, 2007) and reinforced by professional norms and promotional systems. Second, leadership principles and practice cross domains, influencing all other activities and domains within the national security community. Finally, command and control practices directly affect the culture and structure of our organizations through which and across which our projects and initiatives are realized.

It is the unanticipated emergence of "new higher-level systemic patterns or structures functioning according to new laws and consisting of new properties" that characterize complex systems (Jay, 2004) that is so exciting because of what it offers in terms of contributing to our understanding about how novel social structures and processes—indeed, transformation and innovation in social systems—occur. As innovation is fundamentally about generating the novel, research about emergent processes will offer insight into innovation (Goldstein, 2005). Some theorists believe that the bifurcations of self-organization are the primary sources of creativity, diversification, and innovation in systems (Nicolis & Prigogine, 1989).

Even though there is some overlapping between chaos theory and complexity theory, in the study of social systems we are primarily using complexity theory, as it accounts for the capacity of systems to carry information about themselves and their environment and act based on that information, to replicate their ideas at remote sites, and to engage in deliberate adaptive behavior (as well as unconscious adaptation) based on past experiences and anticipated outcomes (Marion, 1999). Although bordering on chaos, complex systems are more stable than chaotic systems. However, complex systems are nonlinear and unpredictable for several reasons. First, they are sensitive

to initial conditions—conditions that can reverberate and amplify through an interactive system to lead to outcomes grossly out of proportion to the initial size and intensity of the cause. Second, several phenomena present themselves as a result of the interaction of agents within the system. Interaction among agents can release potential energy to affect behavior and outcomes in unpredictable ways, first observed by Poincaré and referred to as "resonance." Another phenomenon, correlation, results when two particles collide and their behavior begins to act in synchrony (Marion, 1999; Prigogine, 1996). This essay argues that these social mechanisms help explain what is described in network-centric warfare as self-synchronization, and that it is correlation that offers constructive constraints to the process of self-organization. These properties of complex systems preclude a reductive approach to systems that assumes that with knowledge of most or almost all of the facts governing the constituent parts of a whole, one can control and predict outcomes of the whole system. Complexity argues for a more holistic understanding of systems.

Emergent Leadership

The common conceptualization of leadership is that in which the authority to lead is primarily vested in an individual whom we assume has the ability to predict, plan, and control outcomes. The desirable attributes of the leader associated with this model are based on assumptions of a linear relationship between organizational design, strategy, human behavior, and the desirable outcome of organizational effectiveness; however, these expectations do not capture the reality, nor are they compatible with the nonlinear world in which we live. This conventional perspective views the major functions of a leader to be designing the organization to "fit" the environment, planning the strategy, and hiring the "right" people to effect specific performance outcomes. The perspective about what is effective leadership arising from this viewpoint does not consider the possible effects of interaction and mutual influence among many agents within the organization and throughout the larger system of systems in which the organization operates, frustrating expectations of simple cause–effect relationships. In effect, within the conventional perspective on which most research is based, leaders are viewed as either heroes, in the case of organizational effectiveness, or scapegoats when the outcome is failure, without

consideration of the nonlinear and emergent properties of the situation. (Plowman & Duchon, 2007)

From this new perspective, leadership is viewed as a process and an emergent event arising from dynamic interaction among agents over time (Lichtenstein et al., 2006). One leader may emerge at a particular moment to advance common interests and goals and then recede to let another individual or group lead at another point "*leadership* in complex systems takes place during interactions among agents when those interactions lead to changes in the way agents expect to relate to one another in the future" (Hazy et al., 2007, 7), whether the changes are the result of changing perceptions about objectives or strategy or norms relating to behaviors.

Complexity Science

Although delving deeply into the mechanisms supporting the process of emergence is not within the scope of this essay, some explanation of "singularities" will offer a foundation by which to advance our dialogue. Singularities are the critical points, transition points, or phase transitions, when a disordered state reaches a threshold and undergoes a transformation process of self-organization when previously disconnected elements or agents begin to interact in concert in an ordered pattern. These singularities mark the emergence of order out of chaos.

As the self-organization process may be modeled mathematically, it is possible to configure a visual representation of its behavior—a phase portrait. The trajectory of behavior of the system in time may be traced by a point representing the state of the system along critical dimensions corresponding to the degrees of freedom as it moves in time through phase space. The mathematical powers of computation offer us the opportunity to learn more about systems,—how they change, and how new structures are formed by exploring attractors and bifurcations in the phase portrait.

In the process of self-organization, singularities or critical points are embodied in "attractors" and "bifurcations" in the phase portrait. Attractors act like gravitational pulls to attract systems to their orbit. Leadership in complex dynamic systems is most analogous to a strange attractor. The trajectories of strange attractors, although stable, never repeat themselves and have the capacity to change, diminish in size, or involve a narrower or broader range of beliefs and behaviors in the

social system. Qualities of strange attractors represent long-term behavioral tendencies of a system and are products of nonlinearity and interactivity. Within the leadership realm, they can represent a prevailing ensemble of interconnected values beliefs, ideas, norms, symbols, attitudes, and action tendencies that support a particular leadership prototype (Marion, 1999). Panzar et al. (2007) argue that the challenge of organizations is to simultaneously engage the potential of three types of dynamical leadership attractors—formal leadership, emergent leadership, and shared leadership—to effectively meet the challenges of complex environments.

In his description of the "far-from-equilibrium" phenomenon, by which systems adopt novel processes and structures, Prigogine (1996) discusses the role of bifurcations in thermodynamic systems. A system is stable until it reaches a critical threshold on a path or trajectory between near-equilibrium and far-from-equilibrium called the point of bifurcation, when a critical parameter crosses a threshold. At this point, the system crosses the boundary to a landscape of different attractors available to the system. It is an unstable system until it "chooses" to fluctuate to one of the alternative attractors to regain its stability. Bifurcations are the point in the trajectory when one kind of attractor is transformed into another. What is so captivating about this discovery is that in moving to a different trajectory from instability, the system self-organizes to realize some degree of learning, innovation, and even transformation. This appears to be a mechanism for innovation, radical change, and structural change. Through this process, new levels of order spontaneously emerge in nonequilibirum systems, resulting in greater system capacity to adapt to outside conditions (Marion, 1999; Prigogine, 1996).

Although those holding conventional views of social systems view this instability and these fluctuations as undesirable, effective leaders understand that these "far-from-equilibrium" states might seek to generate learning and new order for the system within this emergent process. Moving from a paradigm of leaders who predict and control for specific outcomes to those who appreciate the generative potential of instability, the question becomes, how does leadership support the potential for learning and the realization of transformation, adaptability, and resilience in an organization or institution?

Command and Control Literature of the U.S. Department of Defense

Linking the broader social science literature with U.S. Department of Defense (DOD) literature is important for several reasons. First, to draw effectively from knowledge created in academic networks we need to integrate the contributions of both communities. The Minerva Initiative, introduced by U.S. Secretary of Defense Robert Gates in 2008, highlights the need for deeper and broader conversations between the DOD community of researchers and analysts and academia to mutually benefit both communities. The military has a great legacy of action research, which can be exploited in the most positive sense to more effectively translate advances in understanding so they may be of use to practitioners.

Alberts & Hayes (2003, 2006) draw from the "edge of chaos" metaphor in their research on edge organizations. In their analysis of the practice and principles of command and control (C2), Alberts & Hayes (2006, 2007) identify three essential factors of C2 in the structures and processes of a given enterprise: the degree of constraint in patterns of interaction, the degree of control in the allocation of decision rights, and the degree to which information is distributed (see figure 1). Alberts & Hayes (2006) argue that, although a traditional C2 might be appropriate for a limited set of conditions, different approaches to leadership ranging from traditional C2 to highly distributed forms of leadership are required to function effectively in the networked environment of the 21st century. This model is a useful tool for practitioners, theorists, and analysts in examining their assumptions about authority and control and in moving toward different models of effective leadership. Alberts and his coauthors apply the term *edge organizations* to those organizations that leverage turbulence by exercising few constraints on patterns of interaction among agents, broadly allocating decision rights, and allowing information to be widely distributed to accelerate rates of learning to maintain competitive advantage.

Alberts, Garstka, and Stein (1999) developed the key tenets of network-centric warfare based on a new mindset about warfare, in which combat power and strategic advantage are achieved by leveraging the advantages of geographically dispersed, network-centric operations to achieve commanders' intent. The authors articulated a process whereby sharing of information among agents effects a high level of shared
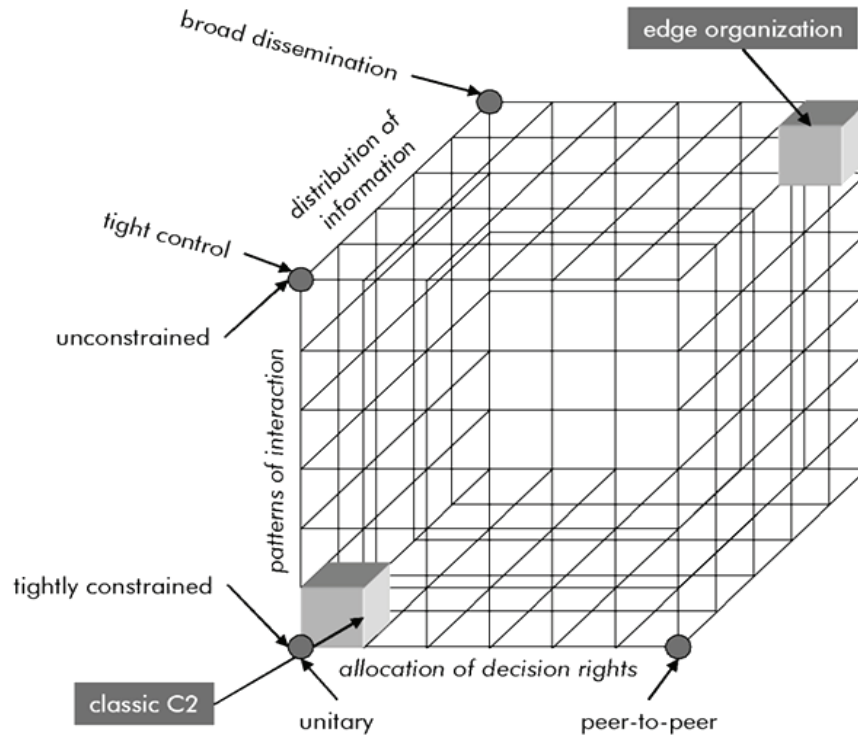
Figure 1: C2 Approach Space (Source: Alberts, 2007)

situational awareness and understanding "that can be exploited via self-synchronization." Several case studies offered some evidence to support the theory (Gonzales et al., 2005; U.S. Department of Defense, 2006).

The author asserts that self-synchronization can often be more usefully understood as an emergent process of self-organization, whereby the phenomena described earlier—correlation and resonance—help explain the mechanisms by which self-synchronization occurs. Correlation can be seen to represent constraint on the system, as it binds self-organizing within behavioral limits structured by, for example, "implicit command intent," as behaviors that adopt a certain level of synchrony and act with some degree of harmony. Resonance describes how potential energy is released when individual agents interact, and could be viewed as the more expansive force that is constrained by the correlation mechanism.

Linking the Cognition of Emergent Leadership to Innovation

Recent advances in social sciences underscore the role of cognition in decision-making, and, by extension, innovation. Boisot and his colleagues (Boisot, 1998, 2007; Boisot & MacMillan, 2007; Boisot et al., 2007) have contributed substantively to our understanding of knowledge processes within and between systems. Rejecting the embedded notion, which is especially trenchant in the world of information and communications technology, that information has a reality totally separate from the social and cognitive processes that give it life, Boisot (2007, 7) fully examines how "[I]nformation only becomes knowledge if it gets internalized and becomes part of the recipient's expectation structure—that is, if it affects the recipient's belief structure, taken as a disposition to *act.*" In the elaboration of his three-dimensional Information-Space, or I-Space, Boisot highlights the nuances of organizational and institutional behavioral patterns that support information processing and knowledge creation by tracing the dynamic behavior of data flows. The three dimensions of Boisot's I-Space capture the forming and structuring of phenomenon, and then the dispersion of information, that characterize agent behavior. The three dimensions are the degree of codification by assignment of perceptual and conceptual categories, the degree of abstraction (structuring the form by reducing number of attributes), and the degree of dispersion of information (Boisot, 1998).

What patterns of collaboration characterize an effective project team, an organization, or even a society? How does the team or organization support or experiment with new ideas? What beliefs do they have about effective leadership? What is their learning curve; that is, what patterns are associated with both their distribution of information and knowledge and their behavioral patterns in terms of rethinking and restructuring ideas, beliefs, and behavior? Boisot and MacMillan (2007) emphasize the importance of the mindset of the leader, entrepreneur, and institution in supporting learning and innovation. Real innovation does not correspond with situations when all the facts supporting an action are known or even exist. As a consequence, to be innovative, there must exist a disposition toward risk to act under conditions of uncertainty, when the justification for acting is based on conjecture and belief, rather than facts, because they are unavailable. As a consequence, important capacities are the

recognition by the agent of the underlying relationship between the type of justification for action and the action itself; the level of awareness and flexibility to distinguish between uncertainty and risk, to deal with uncertainty constructively, and to choose among different levels of risk, dependent on the situation; and an understanding that an agent can influence and shape "plausible and possible" worlds to make them more "probable and actual" (Boisot & MacMillan, 2007). Innovation is integrally connected to effective knowledge management, which balances exploitation of existing capacities with the process of exploitation—the creation of new knowledge.

Leadership Development Framework

Given the high levels of uncertainty, complexity, and volatility existing in the world today, how should we conceptualize effective leadership? How does our understanding of emergent processes, nonlinearity, and the interdependency of systems affect what constitutes effective leadership? How can we develop and support leadership processes that undergird flexible, adaptable organizations with capacities for both competition and collaboration? In the introduction to this essay, the author proposed that a paradigm shift in our understanding of leadership is required—one that is responsive to the challenges of the 21st century and incorporates the knowledge of recent advances in science, especially complexity science. On the basis of material presented in this essay, it is possible to describe a conceptual framework to approach leadership and leadership development that is compatible with both the complexity of the networked and interdependent environment and the challenges it presents to national security.

The leadership development framework (LDF) is grounded in constructive development theory—a conceptual approach firmly grounded in the knowledge that human beings naturally continue to develop through adulthood, progressing through distinct stages. This theoretical framework asserts other tenets, including that development is more than acquiring new information and consists of qualitative changes in the way we know or make sense of the world, that the demands placed on adults frequently surpass their developmental capacities, that development is stimulated through the continuing interaction between the individual and the environment, that individuals are active participants in their own growth, and that an individual's

development, both the enhanced understanding and skills within one's present stage of development and movement from one stage to the next stage, benefits from support for this emergence, extension, and elaboration as a way of knowing and the skills associated with each stage (Popp & Portnow, 2001, 49–52).

The framework is cognitive and interpretive, in that it links action-logic to action. The way we make sense of the world and how we interpret our experience influences our actions. We justify our actions, and we act in ways that we believe will bring about particular results or outcomes based on our map of causal relationships. The relationships between belief and action we espouse may not be the same ones that we, in reality, enact, or we might be unaware of them; nevertheless, the strength of the link between our cognition and action remains the same.

Several theorists have identified specific stages of development characterized by distinct ways of organizing information (cognitive frameworks)—the manner in which individuals construct their experience and knowledge to create meaning. The stages of individual development, called action-logics[1] in the LDF and described in more detail below, correspond closely to the stages of development identified by other development psychologists, including Kegan (1994; Torbert, 1991), Alexander (Alexander & Langer, 1990), Kohlberg (1984), Loevinger (Loevinger & Wessler, 1970), and Wilber (2000). The Leadership Development Profile (discussed below) emerged from Cook-Greuter's theoretical and empirical work to enhance Loevinger's work (Cook-Greuter, 1990, 1999; Torbert et al., 2004).[2]

---

[1]The meaning of the term *action-logic* is somewhat related to the more commonly used term *mindset*. However, this term, coined and defined by William Torbert and David Rooke in their development of the Leadership Development Framework and Profile, more specifically refers to schemas and strategies used by entities (individuals, teams, organizations, and societies) for reflecting on and representing their experience. The term *action-logic* emphasizes the relationship between this logic or organization of reality and the action of the entity. See the following references: W. Torbert, *Action Inquiry: The Secret of Timely and Transforming Leadership* (San Francisco, CA: Berrett-Koehler, 2004); David Rooke and William Torbert, "Seven Transformations of Leadership," *Harvard Business Review*, 2005;April:67–76; and Martin's chapter, "The Schema," in *Complexity: Metaphors, Models, and Reality* (Boulder, CO: Westview Press, 1994)

[2]Examining the overall distribution of developmental action-logic scores from the results of several studies of professional adults in the United States

This essay proposes that the LDF is compatible with what has to this point been referred to as emergent leadership—a perspective that incorporates what we have learned about interaction, learning, change, and innovation in systems from complexity science. The larger framework of emergent leadership incorporates the generative and constructive power of action. Thus, a critical epistemological stance of this approach is that actors not only interpret the reality of their environment but also, in doing so, contribute to the construction of the reality around them. In other words, individuals do not act on a larger reality that exists separately from themselves but, rather, participate in the construction of the system or systems of which they are part through their beliefs, and attitudes and the expression of these ideas in their actions. This is not to be confused with the Newtonian position, which asserts that actors can control their environment in which an assumption of linearity prevails. Nor, in contrast, should this position be conflated with an extreme phenomenological position that posits that the world does not exist separately from our construction or representation of it. The emergent leadership framework, as does the LDF, takes a realist approach to constructivism.

The LDF identifies and describes seven stages of leadership, characterized by an increasingly complex manner of understanding oneself, perceiving the world, interpreting experience, and interrelating with others and the environment: the Opportunist, the Diplomat, the Expert, the Achiever, the Individualist, the Strategist, and the Alchemist. Table 1 distills a large body of literature describing the qualities of each of the seven stages, from the Opportunist through the Alchemist. (More detailed description of each stage are available in Rooke & Torbert, 2005, and Torbert et al., 2004). Some dimensions along which individuals transform are the main focus of their awareness, their perspective on relationships, their sources of satisfaction, their relationship to power, and the valuable contributions they make to an organization. For example, an Achiever welcomes

using the Leadership Development Profile and others highlights the degree to which different developmental theories and the measures associated them are similar. Specifically, the results of different studies conducted in the United States using either the Leadership Development Profile or Kegan's Subject-Object Interview yielded distributions of developmental scores that were almost identical for both sets of studies: 58% of the subjects scored at Expert level or below, and 35% to 36% scored at Action-Logic Achiever, with 6% to 7% scoring at later action-logics (Torbert, *Action Inquiry*).

feedback, is increasingly self-aware, and prefers to work in teams. The Achiever's main focus is on achievement in the near future and planning and making a strategy for the future. A Strategist's main focus is the interplay between visions, strategies, actions, and actual outcomes and is increasingly able to deal with complexity and paradox, as well as being willing to act "outside the box." Each successive later stage reflects a more complex understanding of interdependencies of entities, whether individuals, teams, organizations, or interorganizational systems, as a basis for action, as well as high-level capacities for mutual feedback, sharing power, and temporal orientation. An important dynamic of this model is that with the development to each successive stage, the individual does not abandon the capacity to act from the orientation of earlier action-logics. An individual's self-awareness of their tendencies to think and act in with a particular action-logic, as well as the relationship between the mindset and the action, enables the person to act from a chosen perspective purposefully and with full awareness. In other words, in developing to a later stage, the individual enhances a repertoire of beliefs, attitudes, and behaviors by which to respond to the environment. Relevant to our understanding of organizational transformation, Rooke and Torbert (1998) found a statistically significant relationship between the action-logic of the Strategist and a chief executive officer's ability to lead successful organization transformation.

The leadership development profile (LDP) is the assessment instrument associated with the LDF, developed over the past 20 years through modifications of Jane Loevinger's Washington University Sentence Completion Test through a collaboration of Susanne Cook-Greuter, Dal Fisher, David Rooke, and Bill Torbert. The Washington University Sentence Completion Test is one of the most widely used and thoroughly validated instruments in pscyhometrics (Loevinger 1985; Loevinger & Wessler, 1970; Torbert et al., 2004). The LDP consists of 36 sentence stems that are completed by those taking the assessment. The answers are coded, interpreted, and analyzed in a rigorous process (Torbert et al., 2004). The measure is designed to capture the level of leadership development of the individual by identifying the dominant action-logic of an individual; that is, how the individual interprets their environment and explains their actions.

Action-Logic	Qualities and Capabilities	Strengths	Research Sample at Level
Opportunist	Focus on winning at any price Manipulative, impulsive	Good salesperson Performs well in the short-term	5%
Diplomat	Avoids conflict Respects existing norms	Helps to create harmony in working groups	12%
Expert	Values expertise and logic Seeks efficiency	Productive as individual contributor	38%
Achiever	Effectively achieves goals through teams	Action- and goal-oriented; effective manager	30%
Individualist	Integrates personal and organizational values and goals	Effective in consulting and entrepreneurial ventures	10%
Strategist	Understands interdependencies among systems. Leads with combination of "fierce resolve and humility"	Effective as transformational leaders	4%
Alchemist	Creates opportunities for transformation Simultaneous focus on short and long term	Creates learning organizations Leads society-wide transformations	1%

Table 1: Action-Logics: Seven Transformations of Leadership (Source: drawn from the work of David Rooke and Bill Torbert)

This action-logic, or map by which the individual makes sense of the world, is scalable. In other words, the behavioral tendencies based on a causal map can characterize an individual, a team, an organization, an inter-organizational initiative, or a society. This does not mean that all individuals within a group or organization possess an identical map; however, there exists sufficient coherence and compatibility that a particular action-logic does, in fact, characterize how action is justified and the domination of one action-logic over others. However, alternative action-logics or leadership attractors may exist in the landscape of a system. In addition, for example, the recognition of a great discrepancy between the stated goals and actual outcome of an initiative or strategy of an organization or a nation can lead to a bifurcation, when the landscape of attractors changes dramatically.

The foundational argument of this essay is that maintaining competitive advantage in a network-enabled and interdependent world calls for a new perspective—a paradigm shift in our thinking about leadership and leadership development

Drawing from this framework, the author has identified leadership capabilities required within organizations operating in national security. These capabilities can be applied to individuals, as well as teams and organizations or networked communities.

1. Sufficient cognitive agility to reconcile multiple and diverse mental frameworks (Kegan, 1994; Rooke & Torbert, 1998).
2. Sufficient cognitive complexity to respond and adapt to diverse and changing environmental and internal stimuli. Applying Ashby's law of requisite variety to social systems (Ashby, 1956), individuals, teams, organizations, and societies must have enough variety in their cognitive frameworks to be able to adapt to a range of circumstances. A subset of this capability is to have a high degree of self-awareness, enabling the entity (whether an individual, a team, an organization, or a society) to be able to identify the assumptions being brought to bear relating to particular situations and to understand the limits of their application to act effectively (Alexander & Langer, 1990; Argyris & Schön, 1974; Scharmer, 2007).
3. A worldview consistent with complexity; for example, embracing uncertainty and change as opportunity, learning from diverse points of view, and tolerating differences.

4. Enhanced capabilities for mutual feedback and power sharing (Argyris, 2004; Torbert et al., 2004).
5. An ability to recognize emergent patterns in both social and physical systems (Plowman & Duchon, 2007; Scharmer, 2007)
6. An ability to harness collective intelligence by working in an inclusive, collaborative way to grow communities of trust, including the ability to encourage conversations, enhance connections to share information, and support mutual sense-making (Plowman & Duchon, 2007; Scharmer et al., 2004).
7. An understanding of sense-making and learning processes and how they contribute to an organization's capability for innovation, adaptation, and timely action (Boisot & MacMillan, 2007; Senge, 1990; Weick, 1995).
8. Ability to maintain perspective from multiple temporal realities concurrently; that is, being actively aware of how the past is influencing the present and how current actions might affect the future (Jaques, 1982, 1989; Senge et al., 2005; Torbert et al., 2004).

These capabilities and cognitive frameworks (action-logics) are compatible with an emergent perspective, representing movement toward a different paradigm or, if you will, toward an alternative leadership attractor, and they are captured in the administration of the LDP. There is a growing body of literature and consensus that supports their effectiveness in "leading" complex adaptive systems.

LDF and LDP Compatibility With Emergent Processes

The LDP is one of the few highly validated instruments that are compatible with the conceptual foundations of complexity theory. The framework and profile are consistent with viewing leadership as a dynamic emergent phenomenon in complex social systems, whereby "leadership can be enacted by any interaction in an organization" (Hazy et al., 2007, 2), rather than being lodged within one person or role.

As leaders advance to later-stage action-logics, they acquire higher level capacities to learn, adapt, offer and accept feedback, and share power. The leader's capacity for encouraging conversations and mutual sense-making required for network-enabled operations is emphasized. Acting from later-stage action-logics, individuals and organizations are not fearful or perplexed by complexity, change, or paradox—conditions

characteristic of "far-from-equilibrium" states—but, rather, recognize the generative capacity of these states and seek to use these challenges productively and positively as opportunities for learning and development for themselves, their organizations, and their societies.

Emergent Leadership Action Research Project

The author of this article designed and conducted a pilot project exploring leadership and leadership development that was integrated into the delivery of an elective in Defense Transformation for resident students at the U.S. Army War College during the academic year of 2007–08 and was supported by the Transformation Chairs Network, formerly of the Office of the Secretary of Defense. This study was designed as an action research study (Reason and Bradbury, 2001), in that the "human subjects" acted as full participants in the study to maximize both their learning and development and the validity of the findings using their contributions and insights.

The research objectives were to increase understanding of the relationships between leadership and organizational development and transformation in the context of multinational, interagency, and joint military projects and missions; gain knowledge about how to structure projects and programs of leadership development to support and accelerate effectiveness and transformation at our institutions; and support leadership development of individual participants.

The LDP was the instrument used to assess the leadership development of the participants in the study. The results of the assessment and the debriefing sessions with individual participants, as well as participant observations made by the author as principal investigator during the course of the 10-week course, were used as data sources.

The demographics of the 14 participants are presented in table 2. In summary, it was a small, self-selected group that included both military and civilian U.S. Army personnel. Two of the participants were from foreign military services—one European and another Asian. Ten were colonels, and two were lieutenants. The two civilians had equivalently high ranks in the civilian core. Thirteen were students, and one participant was a faculty member. The elective was taken in the final 3 months of a highly selective resident program for developing leaders at the strategic level in national security. A high degree of trust was

established among the students and between the students and the faculty.

Gender: 10 male/4 female
Military/civilian: 12 military/2 civilian
Of 12 U.S. citizens, 3 were African-Americans
Of services: All were Army
U.S. citizens/foreign fellow: 12 U.S./2 Foreign Fellows
Of foreign fellows, one was European and the other Asian
Age: 40 to mid-50s
Rank: 10 colonel/2 lieutenant colonel/2 civilians, who had had equivalently high ranks in civilian corps
Education: All but one participant had a master's degree
Deployments: At least 6 with recent leadership experience in combat operations

Table 2: Demographics of Participants in Leadership Study

This study was an exploratory, inductive study, rather than a statistical one. The participants were not randomly chosen but were a small group of self-selected participants who, as evidenced by their choice of electives, were interested in transformation and leadership. By virtue of their presence in the highly selective group of resident students at the U.S. Army War College, they most likely demonstrated strong leadership in either field operations or enterprise management within the DOD or the foreign equivalent.

Results of the Study

The distribution of the action-logics is represented in table 3 and is compared with samples representing other populations reported in studies by Torbert and Harthill. In summary, 7% of the study sample scored at the Expert level, 50% scored at the Achiever level, 21.5% at the Individualist level, and 21.5% at the Strategist level. Note that the sample of students, managers, and supervisors represented in the far left column were assessed between 1980 and 1995 and were predominately from the United States. The sample of consultants and

managers were assessed between 1993 and 2006 and were predominately in the United Kingdom. In this simple comparison, we see that the shape of distribution of action-logics remains similar across all samples; however, as the complexity of experience reflected in the sample increases, the top of the bell curve moves to the right, toward later-stage action-logics.

The framework was found to be viable for use in the context of national security professionals, in that the logic of the framework resonated with the participants in the context of their experience. They readily used it to explain the outcomes they had experienced in previous leadership experience and to design strategies about how to address organizational and leadership challenges in their future. The framework seemed to help participants understand their own behavior. In summary, the conceptual framework created a tangible path for development, including the consideration of strategies for their future leadership growth in the context of their next position. This qualitative finding is valuable because the LDP had not been previously been used within the population of national security workers. This pilot project demonstrated that the framework was viable from the point of view that it made sense to them and generated interest in their own development.[3]

We cannot generalize from this very small sample to a larger population; however, on the basis of these results, one can extract a number of insights. Our institutions of national security are, for the most part, producing and rewarding Achievers. Even though Achievers play a very important role in organizations, we need to support the development of the action-logic of Strategists to accomplish the organizational transformation necessary in so many of our institutions. Although Achievers become involved in the crafting of plans and strategies for the future, they tend to focus on achieving shorter-term goals, sometimes forsaking longer-term strategic outcomes. Given the challenges of the 21st century for high levels of collaboration, innovation, learning, and adaptability, institutions need to encourage

---

[3] In ensuing presentations to national security professionals who work in the field and among researchers and instructors who educate this population the framework was similarly received. For example, this was the reception at the 2008 Stability Operations Training and Education Workshop held at Carlisle, PA.

Leadership Development Profile Stage/Action-Logic	4510 students, managers, and supervisors	1556 consultants and managers engaged in development	14 military and civilian leaders in armies (12 in U.S. Army, 2 in foreign armies)
Impulsive and opportunist	4.0%	0.0%	0.0%
Diplomat	11.0%	1.0%	0.0%
Expert	37.0%	14.0%	7.0%
Achiever	30.0%	45.0%	50.0%
Individualist	11.0%	25.0%	21.5%
Strategist	5.0%	12.0%	21.5%
Alchemist and ironist	2.0%	3.0%	0.0%
Total (rounded figures)	100.0%	100.0%	100.0%

Table 3: Distribution of Action-Logics (Source: Harthill, Inc. and Sandra M. Martinez)

and offer support to Strategic Leadership—leadership that is "adept at creating shared vision across action-logics" (Rooke & Torbert, 2005, 71) and can deal with the interrelationships of personal, organizational, national, and international developments. Research has shown that Achievers need to develop through an Individualist stage, in which they question the cultural prescriptions for behavior and the goals and strategies of the organization within which they function and as they seek to reconcile personal, professional, and organization needs. In the context of this framework, we need to support this development of motivated, high-potential leaders to move through a period that is inherently unconventional to reach a higher-level capacity for leadership.

Larger and longitudinal research projects measuring the same dimensions are necessary to answer such questions as, is the U.S.

military leadership in a phase transition? What are some of the emerging characteristics of the merging military or national security leader? What are the factors influencing this transformation? What is the range of variability of leadership development among different military hierarchy, different services, or other constituent groups?

Recommendations

To meet the challenges of the 21st century, our institutions of national security need to effectively engage in multimodal ways of supporting leadership with enhanced capacities for collaboration, innovation, and in general, achieving productive outcomes for systemic interventions at many levels in complex environments.

Our educational institutions play a vital role in meeting these challenges. I recommend curricula for national security professionals that fully integrate tangible and effective programs of leadership development within more traditional academic programs. Several DOD educational institutions are currently designing or implementing hybrid Master's degree and certificate programs that include resident and distance-learning elements in which the institutions integrate this type of leadership development into the curriculum. On the basis of this pilot study and the principles presented in this essay, the recommendations are to use leadership development assessments designed to measure capabilities related to cognitive complexity and effectiveness in complex environments, offer feedback to students in a learning environment in relationships of trust and in the context of the challenges of their current and future positions, and accompany this process with opportunities for reflection to support increased awareness about how participants perceive and structure reality and how this influences their behavior and, ultimately, their effectiveness within their organization and larger network of individuals with whom they interact.

For students to progress, they require opportunities to experiment with new ways of thinking and behaving in the context of their professional and organizational challenges. The academic elements of these programs should include carefully selected content about emergent principles that will contribute to the students' understanding of how complex adaptive organizations function and will offer new meaningful insights about leadership as a process in general, as well as their own perceptions and behavioral tendencies related to leadership.

In addition, the content, assessments, and activities of the program should be linked to the students' understanding of innovation, learning, and transformation in complex adaptive systems. Faculty need to subscribe to a framework that is compatible with the paradigm presented and commit to developing relationships of trust with the students and sharing power in the classroom to encourage learning.

Conclusions

Technological and organizational innovation are intrinsically intertwined processes involving exploration at many systemic levels including the individual, organizational, interorganizational, and societal. Sustaining innovation requires a mindset or action-logic that understands complex adaptive systems and that can leverage advantageously a balance between the exploitation of information and knowledge already possessed with the exploration for new knowledge to achieve desirable outcomes. To maintain competitive advantage, our institutional action-logic and practices need to reflect a high level of complexity about the interrelatedness of systems—more specifically, in this context, the integration of technological, social, cultural, and cognitive elements of the innovation process—drawing from the most advanced knowledge in the physical and social sciences.

To maintain a competitive position and contribute to sustaining both national and international security, we must leverage the creative capacity of our systems, rather than suppress them by unwarranted attempts to control exchange of information and creation of knowledge. In contrast, individuals, teams, and the leadership culture of our institutions need to understand better what risk means in a highly interrelated and complex world. We cannot accomplish these objectives in an interdependent world without achieving a faster "rate of learning" than our adversaries, which involves leveraging the collective intelligence of all our resources. Ready or not, whether we like it or not, the "edge of chaos" is generally where we are operating or need to be functioning. Recently, there seems to be a reluctance to use the term "transformation" within the DOD; however, it seems clear that organizational and institutional transformation is exactly what is necessary to accomplish the paradigmatic shift in thinking and behavior that is required for sustained learning and competitive advantage and for securing the common good.

The individuals and organizational cultures that support thinking at the threshold of complexity we have described require high levels of self-awareness, tolerance for a broad diversity of thought and approach, capacities for sharing power, and a range of temporal orientations and mutual feedback. This essay has presented a framework for conceptualizing these capabilities and some methods and tools for realizing the transformation.

References

Alberts, D. (2007), "Agility, Focus, and Convergence: The Future of Command and Control." *International C2 Journal*, 1(1), 9.

Alberts, D.S. & Hayes, R.E. (2003). *Power to the Edge: Command and Control in the Information Age*. Washington, DC: U.S. Department of Defense Command and Control Research Program.

Alberts, D.S. & Hayes, R.E. (2006). *Understanding Command and Control.* Washington, DC: U.S. Department of Defense Command and Control Research Program.

Alberts, D.S. & Stein, F. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. Washington, DC: U.S. Department of Defense Command and Control Research Program.

Alexander, C. & Langer, E., eds. (1990). *Higher Stages of Human Development*. New York: Oxford University Press.

Argyris, C. (2004). *Knowledge for Action*. San Francisco: Jossey-Bass.

Argyris, C. & Schön, D. (1974). *Theory in Practice: Increasing Professional Effectiveness*. San Francisco: Jossey-Bass.

Ashby, R.W. (1956). *An Introduction to Cybernetics*. London: Methuen.

Boisot, M.H. (1998). *Knowledge Assets: Securing Competitive Advantage in the Information Economy*. New York: Oxford University Press.

Boisot, M.H. (2007). "Introduction," in Boisot, M.H. et al. (eds.). *Explorations in Information Space: Knowledge, Agents, and Organization*. New York: Oxford University Press, 1–14.

Boisot, M.H. & MacMillan, I.C. (2007). "Crossing Epistemological Boundaries: Managerial and Entrepreneurial Approaches to Knowledge Management," in Boisot, M.H. et al. (eds.). *Explorations in Information Space: Knowledge, Agents, and Organization*. New York: Oxford University Press, 48–76.

Boisot, M.H. et al. (eds.). (2007). *Explorations in Information Space: Knowledge, Agents, and Organization.* New York: Oxford University Press.

Capstone Concepts for Joint Operations, version 2.0. (2005). Washington, DC: U.S. Department of Defense.

Cebrowski, A.K. & Garstka, J.J. (1998). "Network-Centric Warfare: Its Origin and Future." *U.S. Naval Institute Proceedings*, 124(1), 28–35.

Christensen, C.M. (2000). *The Innovator's Dilemma*. New York: Harper Business Essentials.

Cook-Greuter, S. (1990). "Maps for Living: Ego-Development Stages From Symbiosis to Conscious Universal Embeddedness," in M.L. Commons et al. (eds.). *Adult Development, vol. 2, Models and Methods in the Study of Adolescent and Adult Thought.* New York: Praeger, 79–104.

Cook-Greuter, S. (1999). *Postautonomous Ego Development: A Study of Its Nature and Measurement*, unpublished D.Ed. dissertation. Cambridge, MA: Harvard University.

Goldstein, J. (2005). "Emergences, Creativity and the Logic of Following and Negating." *The Innovation Journal: The Public Sector Innovation Journal*, 10 (3).

Goldstine, H. (1972). *The Computer: From Pascal to Von Neumann.* Princeton, NJ: Princeton University Press.

Gonzales, D. et al. (2005). *Network-Centric Operations Case Study: The Stryker Brigade Combat Team.* Prepared for the Office of Force Transformation in the Office of the Secretary of Defense by the Rand National Defense Research Institute, Rand Corporation.

Guillén, M.F. (2001). "Is Globalization Civilizing, Destructive, or Feeble? A Critique of Key Debates in the Social-Science Literature." *Annual Review of Sociology*, 27, 235–260.

Hazy, J.K. et al. (2007). "Complex Systems Leadership Theory: An Introduction," in J.K. Hazy et al. (eds.). *Complex Systems Leadership Theory: New Perspectives From Complexity Science on Social and Organizational Effectiveness.* Mansfield, MA: ISCE Publishing, 1–13.

Holland, J.H. (1995). *Hidden Order: How Adaptation Builds Complexity.* New York: Basic Books.

Jay, J. (2004). "Complex Adaptive Systems: Emergent Leadership," Available at http://www.siliconyogi.com/andreas/it_professional/sol/complexsystems/Emergent Leaders.html [Accessed March 23, 2009]

Jaques, E. (1982). *The Form of Time*. New York: Crane Russak.

Jaques, E. (1989). *Requisite Organization: The CEO's Guide to Creative Structure and Leadership*. Arlington, VA: Cason Hall.

Kauffman, S. (1995). *At Home in the Universe: The Search for the Laws of Self-Organization and Complexity*. New York: Oxford University Press.

Kegan, R. (1994). *In Over Our Heads: The Demands of Modern Life*. Cambridge, MA: Harvard University Press.

Kohlberg, L. (1984). *Essays on Moral Development, vol. 2. The Psychology of Moral Development*. San Francisco: Harper & Row.

Kuhn, T. (1962). *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press.

Loevinger, J. (1985). "Revision of the Sentence Completion Test for Ego Development." *Journal of Personality and Social Psychology*, 48, 420–427.

Loevinger, J. & Wessler, L. (1970). *Measuring Ego Development,* 2nd ed. Mahwah, NJ: Lawrence Erlbaum Associates.

Lichtenstein, B. et al. (2006). "Complexity Leadership Theory: An Interactive Perspective on Leading in Complex Adaptive Systems." *E:CO*, 8(4), 2–12.

Marion, R. (1999). *The Edge of Organization: Chaos and Complexity Theories of Formal Social Systems*. Thousand Oaks, CA: Sage.

Martin, B. (1994). "The Schema," in G. Cowan et al. (eds.). *Complexity: Metaphors, Models, and Reality*. Santa Fe Institute Studies in the Sciences of Complexity. Reading, MA: Addison-Wesley, 263–285.

Nicolis, G. & Prigogine, I. (1989). *Exploring Complexity*. San Francisco: Freeman.

Panzar, C. et al. (2007). "The Paradox of Complex Organizations: Leadership as Integrative Influence," in J.K. Hazy et al. (eds.). *Complex Systems Leadership Theory.* Mansfield, MA: ISCE, 305–325.

Plowman, D.A. & Duchon, D. (2007). "Emergent Leadership: Getting Beyond Heroes and Scapegoats," in J.K. Hazy et al. (eds.). *Complex Systems Leadership Theory*. Mansfield, NJ: ISCE, 109–127.

Popp, N. & Portnow, K. (2001). "Our Developmental Perspective on Adulthood," in R. Kegan et al. *Toward a New Pluralism in ABE/SOL Classrooms: Teaching to Multiple "Cultures of Mind*." Research Monograph NCSALL Report 19. Cambridge, MA: National Center for the Study of Adult Learning and Literacy.

Prigogine, I. (1996). *The End of Certainty: Time, Chaos, and the New Laws of Nature*. New York: The Free Press.

Reason, P.W. & Bradbury, H. (eds.). (2007). *The Sage Handbook of Action Research: Participative Inquiry and Practice.* Thousand Oaks, CA: Sage.

Richardson, K. (2008). "Managing Complex Organizations: Complexity Thinking and the Science and Art of Management." *E:CO*, 10(2), 13–26.

Rooke, D. & Torbert, W. (1998). "Organizational Transformation as a Function of CEOs' Developmental Stage." *Organization Development Journal*, 16, 11–28.

Rooke, D. & Torbert, W. (2005). "Seven Transformations of Leadership." *Harvard Business Review,* 67–76.

Scharmer, C. (2007). *Theory U: Leading From the Future as It Emerges.* Cambridge, MA: Society for Organizational Learning.

Senge, P. (1990). The Fifth Discipline: The Art and Practice of the Learning Organization. New York: Currency Doubleday.

Torbert, B. et al. (2004). *Action Inquiry: The Secret of Timely and Transforming Leadership*. San Francisco: Berrett-Koehler.

Torbert, W. (1991). *The Power of Balance: Transforming Self, Society, and Scientific Inquiry*. Newbury Park, CA: Sage.

Transformation Chairs Network. (2009) "Challenges for National Security Organizations and Leadership Development: Trends and Shocks in Complex Adaptive Systems," in Arnas, N. (ed.), *Fighting Chance,* Washington, DC: National Defense University Press.

United States Army *Commander's Appreciation and Campaign Design.* January 28, 2008. Training and Doctrine Command TRADOC Pamphlet 525-5-500, version 1.0. Fort Monroe, VA: U.S. Department of Army Headquarters, TRADOC.

U.S. Department of Defense. (2006). *Network Centric Operations (NCO) Case Study: Task Force 50 During Operation Enduring Freedom*, version 1.0. Abridged Report. Transformation Case Study Series.

Weick, C. (1995). *Sense-Making in Organizations*. Thousand Oaks, CA: Sage.

Wilber, K. (2000). *Integral Psychology: Consciousness, Spirit, Psychology, Therapy*. Boston, MA: Shambhala.

Essay 8

Observer Warrior

An Unwanted Necessity

By Theodore C. Hailes and John Geis

Abstract

The Blue Horizons research project is a series of overlapping, 1-year studies examining the changing strategic landscape created by accelerating technological change. Focused 20 to 30 years into the future, its purpose is to recommend where today's scarce resources can best be invested to ensure that the U.S. Air Force has the right capabilities to meet future challenges. This year's study developed four alternative futures against which to weigh these future capabilities: a peer China, a resurgent Russia, a failed state, and a jihadist insurgency. Among the key consequences identified in this year's study was that decision cycles are rapidly increasing in speed. The traditional observe-orient-decide-act loop is shrinking toward an observe-orient-decide-act point at which future battlefield decisions will have to be made at machine speeds. Although humans will still set the rules of engagement, they will be "on the loop"— monitoring battle execution—rather than being "in the loop"— making all the command decisions in real time. This essay examines the technologies and attendant threats that make keeping that man "in the loop" in many critical situations impossible.

Introduction

From man in the cockpit—to in the loop—to on the loop.

The quality and timeliness of decisions has tested military leaders since the dawn of warfare. An old Japanese Samurai saying that "one should make his decision within the space of seven breaths"[1] captures the importance of time within the decision-making

---

[1] Yamamoto Tsunetomo, quoted by Tsuramoto Tashiro in *Hagakure,* 1716. Yamamoto Tsunetomo was a samurai who, late in life between 1709 and 1716, dictated his thoughts to an apprentice, Tashiro, who published the collections of the samurai teachings and traditions in *Hagakure*, which translates into English as "hidden leaves."

process. Certainly, however, as modern science has taught, time is relative.[2] This is true in both basic physics and warfighting. Time has been, and remains, a critical component of decision-making. Yet as warfare progressed from tribal battles on the plains, where decisions took days or weeks, to nuclear missiles spanning continents in minutes, the necessity for timely decisions has increased.[3] The quality and characteristics of this change are the focus of this essay.

The component parts of any decision-making process have traditionally revolved around the skill of the leader and his knowledge of the terrain, the enemy, the objectives, and the quality of his own force.[4] These criteria have arguably changed little over time. However, in retrospect, what seemed to create great stress and forced rapid decisions in the past seems to be in slow motion compared with the battlefield that will exist within the next decade as the trend line compresses even further the ability to react effectively.[5] It is the thesis of this essay that the time available to make critical decisions is being so compressed that humans may no longer be able to participate, and life-and-death decisions will necessarily become machine-to-machine decisions, with the human involvement limited to an interested

---

[2] For a simplified discussion of relativity, see Michael Fowler, "Special Relativity: What Time is It?" lecture, University of Virginia, 2008. Available at http://galileoandeinstein.physics.virginia.edu/lectures/srelwhat.html [Accessed April 10, 2009].

[3] The Battle of Little Bighorn is illustrative of timescales of 19th-century battle. To engage the Native Americans, General Custer's divisions broke camp at least several days, and in some cases weeks, before the infamous battle of June 25–26, 1876. See W. A. Graham, *The Official Record of a Court of Inquiry Convened at Chicago, Illinois, on January 13, 1879 by the President of the United States upon the Request of Major Marcus A. Reno, 7th U.S. Cavalry, to Investigate his Conduct at the Battle of Little Bighorn, June 25-26, 1876: Q.Q. 979* (Pacific Palisades, CA: Unknown, 1951). This book is a reproduction of the actual court transcripts of the hearings on the Battle of Little Bighorn.

[4] These characteristics are discussed at length in the Custer transcript, with hundreds of pages of testimony devoted to these very topics. Schwarzkopf talks of the same criteria in his discussion of the first Iraqi war. See Norman H. Schwarzkopf, *It Doesn't Take a Hero* (Bantam Books: New York, 1993), 343.

[5] John Geis II et al., *Blue Horizons II: Future Technologies and Capabilities for the Air Force in 2030* (Maxwell AFB, AL: Air University Press, 2009).

observer. The decision-maker will no longer be able to be in the decision cycle but must build and monitor competent systems that will make the decisions for him.

It is necessary, then, to understand the forces at work that alter the time available for decisions. Some factors are obvious. The speed of a weapon can rapidly diminish reaction time. The lethality of a weapon can alter the risk and consequences. Finally, the availability and reduced costs of such weapons can dramatically increase the number of people who have access to these systems.

The speed of communication and our ability to command weapons has rapidly increased. For example, during the Civil War in the United States, it is estimated that the telegraph was able to move thirty words per minute, and this was considered quite revolutionary.[6] By World War II, the radio had increased this speed to around sixty words per minute. In the Gulf War, the communications rate had jumped to 192,000 words per minute, and today it is estimated to be equivalent to 1.5 trillion words per minute—an amount roughly equal to the entire holdings of the Library of Congress.[7] The ability to move so much information to so many people is having a profound effect not just on the military, but also on society at large.[8]

Further, the accuracy of these weapons has become far better with a lethality progression that is no less startling. The U.S. Air Force has calculated that in World War II, it took 1,500 B-17 sorties to destroy one 60' × 100' target. That number was reduced in Vietnam to 176 F-4 sorties to destroy that same target, and by Operation *Desert Storm*, it required just one sortie and one weapon.[9] In the future, unmanned aircraft will have extended loiter time over the target and have single-shot kill of targets no larger than a shoebox. Clearly the implications

---

[6] "Telegraphy." *Encyclopedia Americana*. Volume 26 (Albany, NY: J.B. Lyon and Company, 1920), 342. Most operators were capable of passing 25–30 words per minute during the time of the Civil War.

[7] Martin Brown, "Rapid Knowledge Formation in an Information Rich Environment." Paper presented at the 2004 Command and Control Research Technology Symposium, San Diego, CA, June 15–17, 2004.

[8] This speed issue is expected to get even worse as computer processing approaches and eventually passes that of the human mind. See Ray Kurzweil, *The Singularity Is Near* (New York: Penguin Books, 2005).

[9] A discussion of increasing lethality over this period is in Brigadier General David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare*, (Arlington, VA: Airpower Education Foundation, 2001), 8.

for these advances are vast, and the United States will not have a monopoly on these systems. That the enemy will have similar capability obviously places great pressure on operational and tactical planning and can readily create actions faster than humans can generate responses. This becomes the crux of the problem.[10]

When these three characteristics are combined, which is exactly what is occurring today, the threat substantially increases, and the time to react substantially decreases. Of particular interest then is to how to grapple with the underlying forces at work creating this challenging mix, illustrate how they affect the speed of decision-making, and then define the new role of the leader in the overall process. The leading element creating such changes is the exponential growth of technology and the increasing rate that new systems are being introduced to the battlefield.

Although its essential nature and purpose may remain the same, war—what it is, how it is waged, its participants, and its effect on the state and the state system—is changing. In the first quarter of this century, the world is witnessing what amounts to a change in the physics of war. The relative importance of matter, energy, time, and information are all being transformed by emerging technologies. We are living in a messy interregnum period between a true Information Age and the rapidly passing Industrial Age. Cyber, which exists in a nanosecond world, is being slammed into an industrial-bound system, and it simply is not working.[11] In just the last half century, decision transaction rates have moved from days in World War II, to 20 minutes in the Cold War (time of flight for intercontinental missiles), to a current 4-minute cycle based on missile defense, and soon, war at

---

[10] This argument is based on the decreasing cost of technology, an exposition of which can be found in: General T. Michael Moseley, *Blue Horizons 2007 "Horizons 21" Project Report*, (Maxwell AFB, AL: Air University Press 2008).

[11] The prediction that the Information Age would clash with the Industrial Age has been made by many authors. Alvin Toffler wrote a series of books that detail the likely implications of the transition to a new era: Alvin Toffler, *The Third Wave: The Classic Study of Tomorrow* (New York: Bantam Books, 1980); Alvin Toffler, *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century* (New York: Bantam Books, 1990); Alvin Toffler and Heidi Toffler, *War and Anti War: Making Sense of Today's Global Chaos* (New York: Warner Books, 1993).

electronic speeds in the domain of cyberspace.[12] Trying to insert people into this decision loop is becoming increasingly difficult, yet the expectation still exists that the human must stay in the loop.

In a few aspects, a world already exists in which humans have been taken out of the decision loop; computers are now protected by antivirus and antispyware programs that act in milliseconds. Human intervention is impractical, as the speed of a virus or malware intrusion in a computer system is so fast that it is impossible for a human to sense the intrusion and react to stop it before the malicious software code is already loaded on the system. As a result, names like McAfee, Symantec, and Norton have become household words around the world, and the defense of most computer systems is now automatic. These same trends will spread rapidly throughout the military environment, moving—by necessity—more decision-making authority to machines.[13]

In attempting to cope with exponential change, the risk of making poor decisions increases dramatically. This is an inevitable effect of linear thinking and will necessarily create surprise.[14] Historically, surprise, in turn, has created the requirement to scrap existing concepts and programs, as well as decision-making processes, to meet the changing environment.[15] Surprise is a natural outcome of rapid change. That the rate of technological change is increasing every year certainly suggests that surprise will be a major component of the environment for

---

[12] The premise of the U.S. Theater Ballistic Missile Defense, to include the Airborne Laser System and the Intercontinental Ballistic Missile Defense Programs, is to intercept these missiles in the boost phase. This phase lasts 1–3 minutes for a Theater Ballistic Missile and 3–5 minutes for an Intercontinental Ballistic Missile. Dean A. Wilkening, "Airborne Boost Phase Ballistic Missile Defense," *Science and Global Security*, 2004;12:1–67

[13] Kurzweil. *The Singularity Is Near.*

[14] Ibid., 4. Kurzweil acknowledges that this argument was made previously in another form by Douglas Hofstadter, who argued are brains are too weak to even understand themselves. See Douglas Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid* (New York: Basic Books, 1979). Diagram is derived from Moseley, *Blue Horizons 2007 "Horizons 21" Project Report.*

[15] Lorber has analyzed several instances of this type of surprise in military operations. Either systems and/or doctrine must be scrapped or the side that adapts to the technological change loses in battle. For a detailed description of how and why this occurs, see Azriel Lorber, *Misguided Weapons: Technological Failure and Surprise on the Battlefield.* (Washington, DC: Potomac Books, 2002).

future leaders. The essential issue is that the human brain works in a linear fashion. This means that the more predictable the future is, the better the brain can deal with the issues presented. Because technology is on an exponential curve, the rate of change caused by new systems will be increasing, increasing the uncertainty of the future. The result is that, whereas in 1850 a 50-year planning horizon was not unreasonable, today a 5-year horizon is challenging. A point will be reached in the not-very-distant future at which the only surprise for a leader will be that he or she is not surprised (figure 1).
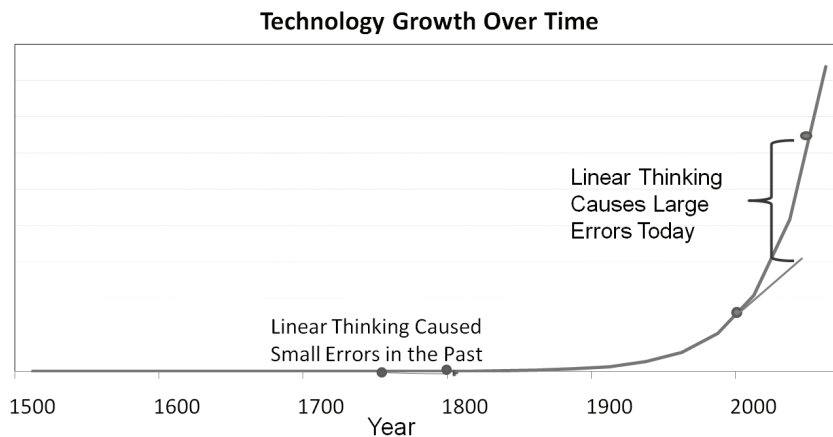
Technology Growth Over Time

Figure 1: Effect of Exponential Change on Linear Decision-making

Modern military weaponry is becoming increasingly remote, robotic, cheap, small, and swift.[16] Nanoscale particles, photons moving at the speed of light, molecular manipulation of the biosphere and life within it, the ability to create autonomous intelligent machines, and the replication of these machines in large numbers and at small cost all suggest major changes in war.[17] It may no longer be about conquest

---

[16] This is obvious in the domain of cyberspace, where the weapon of choice is a computer chip with less than 100 nanometers of transistor spacing. It has been true in other domains as well. In fact, Secretary of Defense Robert Gates recently chided the Air Force leadership publically for not moving swiftly enough in this direction. U.S. Department of Defense News Transcript, "Secretary Gates Remarks at Maxwell-Gunter Air Force Base, Montgomery, Alabama," April 21, 2008, http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=4214 [Accessed April 13, 2009].

[17] Author discussions with members of several Air Force and U.S. Government laboratories between August 2008 and April 2009.

involving large numbers of people engaged in precision, kinetic kill, but increasingly a continuing contest among machines that are nonlethal, nonkinetic, very precise, and/or volumetric (i.e., wide-area oriented) conducting attacks at great distance over long time periods, yet requiring decisions in milliseconds.[18]

Everyone can play. The power of these emerging technologies is such that they can empower the weak and dispossessed to exert an inordinate effect. Some of the key forces driving technological change are societal demand, scientific discovery, corporate profits, ideological desires, and state and non-state envy and hatred of the "have" nations. These factors, not simply U.S. preferences, ensure progress for good and ill in warfighting technologies. These are available with increasing frequency and ease as reliance on commercial off-the-shelf technology grows.[19]

All of these forces make recapitalization of people and expertise paramount. Accelerating technological change necessarily demands significant procedural and organizational change.[20] The importance of educating and organizing the force to create an agile, adaptive, learning organization capable of contending with the array of adversaries and the pace of technological change that will challenge everything in the future cannot be overstated. Leadership is critical, and the skills demanded of that leader will require a fundamental understanding of rapid change and the willingness to alter processes that allow a more automated battlefield running at machine speed. The chief of staff of the U.S. Air Force has launched a multiyear research effort called Blue

---

[18] Geis et al., *Blue Horizons II.*

[19] This process is enabled by decreasing costs of computer processing, ubiquitous access to geospatial location data, and the increasing number of weapons available via global arms merchants. For trends in computer processing and its associated costs, see Ray Kurzweil, *The Age of Spiritual Machines: When Computers Exceed Human Intelligence.* (New York: Penguin Books, 1999). Satellite pictures that once cost a nation millions of dollars to receive are now available for free on Google Earth or can be purchased for as little as £12. One can even get multispectral images from the European Space Agency; http://www.spotimage.fr [Accessed April 13, 2009].

[20] Lorber, *Misguided Weapons.*

Horizons to specifically tackle these issues from an air force perspective.[21]

Blue Horizons: Where the Ideas Came From

The concern about the role of technology is decision-making is not new; it has always been understood in the most general way. However, acknowledging influence and truly understanding effect are very different things. The Blue Horizons program provided an opportunity for extended research into the changes wrought through technology on the air force in 2030 and beyond. The ongoing process has illuminated many of the darker corners and provided, if not answers, a far clearer understanding of the challenges decision-makers will face in the years to come. Focusing on leadership and decision-making in general was never a specified task for research, yet it kept surfacing as a key component of the recommendations made, thus identifying the importance of this nontechnological issue. The journey taken to arrive at these conclusions over 3 years is worth covering, as it provides the basis for and validation of the conclusions to be presented.[22]

The thesis for the first Blue Horizons Study was to evaluate the effect of exponential technological change and to extrapolate trends identifying capabilities that advance or constrain air power. Four critical areas of scientific research were selected to test the hypothesis for accelerating change: nanotechnology, biotechnology, directed energy, and cyber. A brief summary of the conclusions from this report follows.[23]

- All boats rise on a rising technological tide. Maintaining superiority will become more difficult but is possible.
- The key to achieving and maintaining lasting superiority that cannot easily be duplicated by adversaries lies in the integration of information, air, and space with the attendant investment in basic research.

---

[21] Memorandum between General John D. W. Corley, U.S. Air Force Vice Chief of Staff, and Headquarters U.S. Air Force Research Management, dated May 17, 2006.

[22] Ibid.

[23] The conclusions follow from the final study report. See Moseley, General T. Michael, *Blue Horizons 2007 "Horizons 21" Project Report.*

- Information is no longer a staff function but an operational one. It is deadly as well as useful.
- Superiority may derive as much from improved thinking about the employment of current capabilities and the rapid integration of existing technologies as from the development of technological breakthroughs.[24]
- Courage and confidence in technology and our ability to deploy it quickly will enable many of the current missions performed today by manned aircraft to be performed in the future by uninhabited vehicles and space systems.[25]
- The revolutionary information technologies of the future are so fast moving that they suggest the need for dramatic changes in planning, budgeting, and acquisition if we are to continue to compete successfully.
- Increasingly, the U.S. Government will both voluntarily relinquish being the owner of militarily relevant technologies and become a user, licensee, and lessee of commercially developed systems with military applications.
- A revolution in military education will be required if we are to achieve a revolution in military affairs.

The results from the first Blue Horizons study established the nature of exponential technological change and provided illustrations of the game-changing aspects of future technology. It also introduced a nontechnological area that is of considerable interest: the changing nature of command relationships and the ability and manner for leaders to control the battlefield.

Blue Horizons II had the task of building on the previous year's study and "develop[ing] a prioritized list of concepts and their key enabling technologies that the U.S. Air Force will need to maintain the dominant air, space and cyber force in the future."[26] The study started with two key premises: first, that a short list of key technologies would enable a large percentage of future concepts/systems to be developed, and second, that preferred systems and underlying technologies would

---

[24] The first excursion from technology to leadership issues.

[25] Dramatically altering the role of man in the decision loop

[26] Task received from Air Force Chief of Staff General T. Michael Moseley. Study purpose was confirmed by the authors in meetings with Air Force Deputy Chief of Staff for Plans and Programs Lieutenant General Raymond Johns.

vary with the type of warfare.[27] The results from the study were supposed to allow the air force to focus its limited research and development dollars on the areas that would give the most value for the investment.[28] As often happens, what the research generated was results and direction contrary with the extant expectations for the future.

To understand the results, a brief description of the study format is necessary. The researchers were tasked to evaluate the effectiveness of fifty-eight future weapons systems in 2030 and to examine the underlying 172 technologies necessary to bring those systems to fruition. To accomplish that goal, four teams developed alternate futures in 2030 that would act as the testing ground for the new concepts. The four worlds developed were based on the U.S. National Security Strategy[29] and included a Resurgent Russia, a Peer China, a failed state (Nigeria), and a well-financed and well-connected jihadist insurgency. Each world was designed to create different challenges and threats for the U.S. Air Force. A different value-focused thinking model was developed for each world, enabling each weapons system to be scored against the challenges in each world and allowing for the creation of a prioritized list of future systems that performed the best across all four alternate futures. The study then mapped the list of 172 mutually exclusive, yet comprehensively exhaustive, enabling technologies to the fifty-eight concepts[30] and then used a linear algebraic model to quantitatively score the enabling technologies. The research results contained a few surprises.

- The synergistic effects of the underlying technologies were such that no short list for investment could be developed. The effect of nanotechnology, computational power, biotechnology, chemistry, and physics were so interwoven that a lack of research in any one area would disable the fielding of a large number of future systems or concepts. Future science and

---

[27] Geis et al., *Blue Horizons II.*

[28] Meeting between the authors and Lieutenant General Johns.

[29] George W. Bush, *The National Security Strategy of the United States* (Washington, DC: The White House, 2006).

[30] Full methodological details can be found in John Geis II, "Toward Blue Horizons," paper presented at Exploring the Past; Anticipating the Future: The 50th Annual Convention of the International Studies Association, New York, February 16, 2009.

        technology investment is required across the whole of the science and technology enterprise.

- Of equal surprise was that the capabilities required for major state-on-state conflicts are mostly the same as those required for counterinsurgent and irregular warfare. In short, at least for the U.S. Air Force, the notion that if you prepare for the worst-case scenario of major state-on-state conflict, the lesser cases will be covered, appears to be correct.
- The last point, germane to this essay, was that technologies are creating systems that were becoming increasingly unmanned, remote, small, fast, and very lethal, requiring a robust ability to predict, command, and control the battle space.

Blue Horizons: Proofs

The reality of exponential technological change, with its attendant implications for the future, are well understood today, but this was not the case just a few short years ago. Friedman and Kurzweil have altered the thinking and validated the implication of rapidly changing technology.[31] There is now a host of books and substantial scientific work that cover this theme well and that established the legitimacy of accelerating technological change.[32] Exponential change, ranging from such innocuous devices as the computer and color television to the Internet-enabled iPhone, has become part of our everyday lives.

Yet understanding the consequences of such change is far more subtle, although equally important. These technologies are altering the calculus of war and, more to the point, challenging future leaders' ability to act and direct actions. The increasing capacity to move

---

[31] Thomas Friedman, *The World is Flat*; Raymond Kurzweil, *The Singularity Is Near*; and *The Age of Spiritual Machines.*

[32] Examining scholarly works alone, several hundred sources are available on the accelerating nature of technological change, with over 180,000 works written on technological change itself. Technological change is now so critical that the American Political Science Association recently initiated a new professional journal directly related to this topic, the *Journal of Information Technology and Politics*. One of the authors is among this journal's reviewers. Another section of the association is exploring the effect of science, technology, and the environment on politics. See http://www.apsanet.org/content_4596.cfm [Accessed April 14, 2009].

information, and the increased precision and lethality of the weapons discussed earlier, are but two examples of this phenomenon.

Whereas demonstrating that technology is creating rapid change is relatively straight forward, delineating the first-, second-, and third-order consequences of such systems is more difficult. Applying these consequences to decision-making, however, is imperative. To that end, it is helpful to highlight several of the salient points from the Blue Horizons program that will end up influencing decision-making. The overall conclusion of these studies is that exponential change has created a globalized world that, at least technologically, is leveling the playing field.[33] Further, the U.S. Government is now a relatively small player in the science and technology world, where well over 70% of U.S. investment in basic research is now in the hands of industry and academia—and this is a worldwide phenomenon not limited to just the United States.[34] The result of this proliferation of technology has made systems smaller, cheaper, and more capable on a global basis, which is empowering nontraditional actors reducing available reaction times, and, as was demonstrated above, increasing the likelihood of surprise for the United States.

Blue Horizons: The Consequences of Technology for Decision-making

The advances in physics and chemistry are driving the introduction of entirely new concepts that have moved from the macro Newtonian world to a far-more-complex world of quantum affects. As a result of quantum pairs, adversaries will soon have access to "unbreakable encryption," which may make intelligence gathering far more

---

[33] For the effects of globalization, there are many studies beginning with Walter Wriston's seminal work, *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World* (New York: Charles Scribner's Sons, 1992).

[34] In 2004, the U.S. Government spent $20.26 billion on basic science and technology research. Industry in the United States spent $208.3 billion in the same year. Further, nearly 70% of global research and development is outside the United States. In 2004, Asia spent approximately $249 billion on research, and the EU-25 roughly another $210 billion. Thus, these continents nearly spent double what the United States spent before South America, Canada, Mexico, Australia, and Oceana are included. See National Science Foundation statistics. Available at http://www.nsf.gov [Accessed April 14, 2009].

difficult.[35] Nanomaterial coatings can make materials stronger, lighter, and/or more impervious to outside materials.[36] Precise placement of individual molecules and/or atoms now allows the creation of carbon nanotubes (see figure 2) and the building of designer molecules. The former have the potential to radically improve computer speeds, with shorter computer transistor spacing using super- or near-superconducting materials. The latter means that the world may soon enter an era of designer genes—a world with designer pathogens. The nature of the sciences of bio- and nanotechnologies is that the laboratories needed to create these materials are small: They can fit in an average garage. This means that in the future, the power enabled by these technologies will no longer be only within the purview of the nation-state, but also of the group and individual.[37]
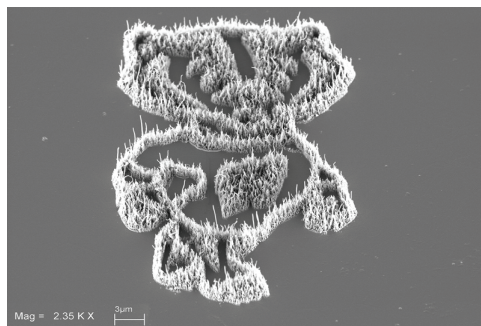

Figure 2: Carbon Nanotubes Placed to Create a Picture of "Bucky Badger"[38]

---

[35] Roland Pease, "Unbreakable Encryption Unveiled," *BBC News*, October 9, 2008, http://news.bbc.co.uk/2/hi/science/nature/7661311.stm [Accessed April 14, 2009].

[36] Nanophase Technologies recently announced coatings that improve resilience to radiation, including ultraviolet, and improve the strength of the materials to which they are applied. These coatings have become ubiquitous in other applications, including in wrinkle-free and stain-resistant shirts. Nanomaterials have the capacity to significantly change the properties of the base material to which they are applied. http://www.ceramicindustry.com/Articles/Products/23c43d89dd9c7010VgnVCM100000f932a8c0 [Accessed April 14, 2009].

[37] Geis et al., *Blue Horizons II.*

[38] Created by Roger Hamers, Chemistry Department, University of Wisconsin–Madison. AIP Industrial Physics Forum, Boston, MA, November 17, 2006. Each carbon nanofiber is less than 75 nanometers in diameter. For

These changes are turning the calculus of war on its head. In the past, conflicts of high consequence were infrequent—even rare. Only major global conflagrations had the potential to cause massive casualties or the destruction of a state, and events like World War I and World War II were uncommon. As we move forward in time, and as these technologies continue to mature, terrorist attacks and events triggered by small groups may become very high consequence events (figure 3). The result is change. Warfare, which has historically followed the diagonal gray line, may soon find itself off of its historic position, near the upper-right-hand corner of this diagram, where non-state actors have the power to greatly affect our world. This has the potential to greatly increase the incidence of surprise and complicates the decision-making process immeasurably.
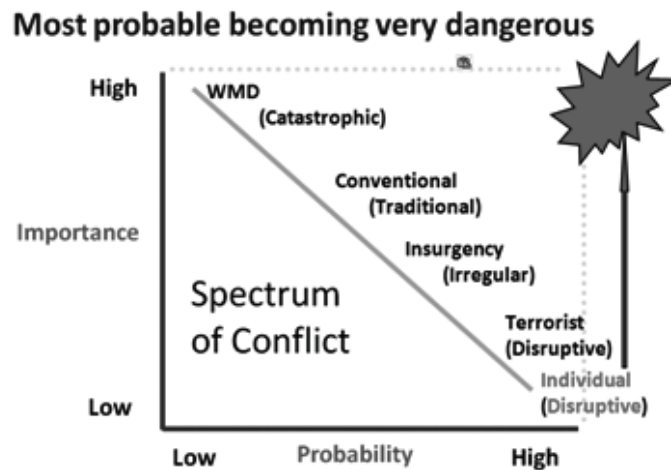

Figure 3: Warfare is Moving off the Traditional Plot of Conflict[39]

Decision-making in This World: The OODA Loop

These technological concepts actually will affect the decision-making cycle. A movement away from the decision-maker being in direct control and toward a scenario in which the decision-maker is

---

size perspective, over 9,000 of these nano-badgers will easily fit on the head of a pin without touching each other.

[39] General T. Michael Moseley, *Blue Horizons 2007.*

only indirectly in control is likely. Although war is—and will remain—a contest of human will, machines will likely control many future engagements. What is clear with the increasing power of future weapons is that whoever can make valid decisions the fastest will have a significant operational and tactical advantage. Speed will increasingly be an important facet of warfighting.
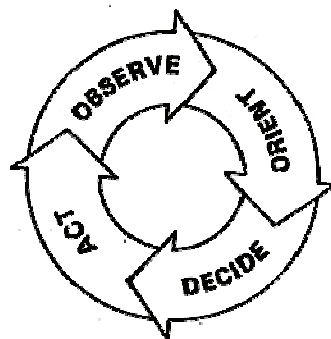

Figure 4: John Boyd's Observe-Orient-Decide-Act Loop

One of the most useful architectures to model this decision-making—the OODA loop—was created by U.S. Air Force Colonel John Boyd.[40] Describing the process as a loop emphasizes the recurring nature of the decision cycle and emphasizes the importance of the time from the point of observation to the point at which a force is able to act (see figure 4). The goal is to have a loop shorter in time than one's adversary—what Colonel Boyd referred to as "getting inside" the opponent's loop. The logic is simple, and the concept has stood the test of time.

New systems coming to the battlefield will dramatically alter the speed with which information is provided, how deeply it is fused, and the alacrity with which a response can be executed. There are innumerable subtle forces that can alter the speed and responsiveness of the loop. The number and type of adversaries on the field, the cultural/political context of the enemy, political constraints from the home front, and the complications that arise from joint and combined

---

[40] The discussion comes from John R. Boyd, *A Discourse on Winning and Losing* (Maxwell AFB, AL: Air War College, August 1987); and Grant T. Hammond, *The Mind of War: John Boyd and American Security* (Washington, DC: Smithsonian Press, 2004).

operations are but a few. All these present challenges that can impede the ability of the leader to plan and execute a task.

Yet the introduction of computer processing and human behavioral algorithms will soon yield predictive awareness—the ability to anticipate an adversary's actions on the battlefield.[41] As other new systems come online, they too will compress the decision cycle, shrinking the OODA loop to, quite literally, a point in time.[42] It is this compression that will force the human out of the decision process and dramatically alter the places in which human involvement will occur when employing weapon systems. It will no longer be an OODA loop but an OODA point. The cyberworld is already working at machine speeds that preclude human involvement in the decision process.[43] It is important to explore this phenomenon by discussing a few systems that will likely mature in the 2030 time frame and evaluating the second-order consequences of those technologies on the decision-making process.

In the observe phase of Boyd's model falls much of what is currently labeled intelligence, surveillance, and reconnaissance. For millennia, leaders have depended on sensors consisting of their eyes and ears—in short, their basic senses—to observe. As warfare increased in complexity and lethality, commanders found it necessary to expand the means for gathering information and developed systems that extended the range of their senses. The telescope and the telegraph enabled sharper vision and faster movement of data, which over the years enabled faster ways to move massive amounts of knowledge. In the fighter pilot world of World War I, the axiom, "first to see—first to kill" prevailed. Later, radar expanded this range further, enabling anticipation of attacks. In the last 60 years, the introduction of new

---

[41] Although this awareness may not be perfect, great strides are possible in the near term. See Robert A. Piccerillo and David A. Brumbaugh, "Predictive Battlespace Awareness: Linking Intelligence, Surveillance, and Reconnaissance Operations to Effects-Based Operations," 2004 Command Control Research and Technology Symposium, San Diego, CA, June 15–17, 2004.

[42] Geis et al., *Blue Horizons II.*

[43] As discussed earlier, this is how the antivirus software on a computer works. Because the human is too slow in his/her reaction time to incoming malware or virus software, the computer executes human intent (keep the computer free of interfering software), usually completely without human intervention.

sensors created from technological advancements has vastly increased the range, precision, and breadth of information from which decisions are derived.[44] Technology, by reducing the size, weight, endurance, capacity, and cost of intelligence, surveillance, and reconnaissance systems, has moved the sensors from space down into the hands of the lowest echelons of our combat forces, making information available more quickly and to more people than ever before. As long as nothing derails the technological innovation process, by 2030, commanders will have access to improvements that will be five to ten times better, which will have implications for how wars will be fought and who (or what) will be making the decisions.

New intelligence, surveillance, and reconnaissance methods, programs, and systems will soon be making their way into the battlefield. One example at the tactical level is a nanoscale sensor network that covers the battle space with thousands of tiny sensors that detect and locate targets, assess behavior, and report "live" movement and change. They will work in the visible or infrared band, sense movement, detect the presence of chemicals or bioagents, and generally make the battlefield "transparent." This will provide the capability to move against multiple small, fleeting targets requiring very fast reaction to be successful.[45]

In the orient phase of the OODA model are even more startling systems defying many expectations of what can be known. Several programs are already underway, most starting with sophisticated computer data-mining processes that will assess and fuse vase amounts of information and turn it into executable knowledge. These will be combined with cognitive approaches that will move and display this

---

[44] In fact, the totality of the information from satellites, backscatter radars, and airborne UAVs is already global.

[45] Fabrication of nanosensors will soon be reality. See Vincent T. Jovene, *Next Generation Nanotechnology Assembly Fabrication Methods: A Trend Forecast*, Occasional Paper 64 (Maxwell AFB, AL: Center for Strategy and Technology, 2008). The use of these smaller and more ubiquitous sensors will enable greater visibility on potential targets. For more on this topic, see Beth M. Kaspar, *The End of Secrecy? Military Competitiveness in the Age of Transparency*, Occasional Paper 23 (Maxwell AFB, AL: Center for Strategy and Technology, 2001); Kirk M. Kloeppel, "Pesky Critters," and James M. Abatti, "Small Power: The Role of Micro and Small UAVs in the Future," in *Netted Bugs and Bombs: Implications for 2010*, Marsha J. Kwolek, ed. (Maxwell AFB, AL: Center for Strategy and Technology, 2005).

knowledge in innovative ways. As trust in these systems grows, so will the drive to allow them to not only assess and predict but also to act. These systems will fuse air, ground, space, and cyber information, and they will mix these data with cultural, political, and geographic information, all to achieve a constant "knowing" of the adversary. The social software existent today provides only a hint of what will be accomplished over the next 20 years. These systems will allow for continuous evaluation of red, blue, and white forces, analyze capabilities, and assess intent.[46]

If computers enable orientation, then the next steps in the loop are those of decision and action. In the area of cyberspace, computers already decide when to take some protective measures. As discussed earlier, most computer operators use a machine to execute the human intent of protecting the hard drive, and so will it be with future combat systems. As the fusing of data becomes better, computers will be able to recognize targets and threats with the same precision as the humans who now man the combat systems. Thus, in both decision and action, the fundamental question for the future is whether to let the computer engage the target on its own. Just as this is already happening on almost every electronic device, this practice will soon migrate to other domains as well.[47]

In the action process, newer and faster weapons will shorten the loop even further. Directed energy weaponry, such as ground-based lasers relayed to the target via space-based mirrors, and hypersonic missiles and aircraft will shorten the targeting sequence to timescales eventually measured in fractions of a second.[48] As Boyd points out, being able to get inside an opponent's OODA loop is of enormous tactical advantage. When the entire cycle shrinks to well under a minute—perhaps even to fractions of a second—it has shrunk to a point. When this occurs, humans can no longer be allowed to remain "in the loop," as they would slow this process to a level at which an opponent would gain significant, perhaps even decisive, tactical

---

[46] Among the programs that will achieve this are those in the area of predictive battlespace awareness, cited earlier.

[47] John E. Marselus, "Who Pushes the Pickle Button?" in *Netted Bugs Bombs.* See also, Geis et al., *Blue Horizons II,* in which some of the top-rated systems, including "Pathfinder," have autonomous attack capability.

[48] John Geis II, *Directed Energy Weapons on the Battlefield: A New Vision for 2025*, Occasional Paper 32 (Maxwell AFB, AL: Center for Strategy and Technology, 2003). Also, Geis et al., *Blue Horizons II.*

advantage. Although it may not be a desired outcome, placing the human in the position of monitoring the execution of this cycle may become a future necessity.

Conclusion

Being able to effect change on a molecular/atomic scale, using photons and electrons, navigating both outer space (our universe) and inner space (ourselves), and being able to fight and communicate "at the speed of light," changes the distribution of power and threatens traditional military doctrine. That reality will alter combat waged in air, space, and cyberspace. To compete successfully in this radically altered environment will require a new way to prepare and immerse leaders in the new technologies and new ways to execute their plans.

The dangers created by the accelerating introduction of new and powerful technologies are substantial. How those technologies will be integrated and employed, and their ramifications, will tax future leaders. The hardest piece for most to grapple with is the question of who or what will be making the combat command decisions in the future. The trend lines are clear: As the complexity and risks of new technologies vastly increase on the battlefield, the ability of leaders to make effective and timely decisions will decrease. The decision loop that once played out over days, weeks, or even months will be compressed into fractions of a second. This is already true in cyberspace, and will soon be true in other areas of the spectrum of combat. As new weapons with mass effects become common through the introduction or expansion of nano-, bio-, and nuclear technologies, leaders will have reduced time to observe events, orient themselves, decide on a course of action, and act. This process will, of necessity, be given over to machine interfaces. Although that moment has yet to arrive, it is visible on the horizon, and dedicated thought, debate, and identification of the critical questions of how best to make this transition are imperative.

The easiest question to answer is whether science and technology can create these new systems. After 3 years of research, the answer of the authors is "yes." On that, the research is clear.

There are areas that require further work, however, and these are the harder questions to answer. Yet time is limited. We must begin to examine questions such as, What are the ethical issues of allowing machines to take lethal action? Who does society hold accountable if a

machine makes a wrong decision or, even worse, commits a war crime? How reliable is machine decision-making in a complex world? Can machine intelligence handle the nuances of political and cultural differences? The hardest question of all may be a very human one: How will humanity deal with such intelligent systems, and how will they deal with us? There are excellent studies and books starting to fill the shelves with thoughts, predictions, and horror stories of that world in 2030. The sooner the debate starts, the better the result and the less probable the horror scenarios. The shift from being the man in the cockpit to being the man in the loop to being the man on the loop appears to be inevitable. The necessity for machine speed may be unwanted, but it cannot be avoided. Those nations that accept and prepare for this reality will have a substantial advantage in the world of 2030.

A Reevaluation of the "Kill the Leadership" Doctrine

By Torsten Björkman

Abstract

The elimination of leaders has a long history. Analyses of such assassinations is a favorite among both historians, and "if-not historians"(What would have happened if Count von Stauffenberg had assassinated Hitler?).

The "kill the leadership doctrine" takes on new meaning when applied to asymmetrical warfare. "Anarchist terrorism" targeted the leaders of the establishment. In "suicidal terrorism," interest is lost in killing leaders and retargeted on ordinary people, but for counterinsurgency there is no killer to be killed in suicidal terrorism. Finding the leaders of the perpetrators becomes a paramount concern. The leaders of terrorist organizations know this and are developing defensive strategies to improve the capability of coping with the loss of leaders.

Leavitt's diamond is used as a frame of reference. The relative importance of people, process, organization, and technology is evaluated. The caliber of who is killed certainly matters. When someone is killed is extremely important, in particular in relation to process. The technologies have evolved, mainly strengthening the means of the perpetrator. Organization is estimated as the variable with the most potential in this context. At the end of the essay, the focus is on organizational transformation, and the relevance of Leavitt's model is evaluated.

Introduction

Force transformation is to a large extent technology driven. The emergence of new asymmetrical adversaries—terror networks like Al-Qaeda and the Taliban—represents a second social and cultural challenge and driver to force transformation. What does it indicate that Bin Laden has not yet been caught or killed? Are these new adversaries in a traditional sense good at protecting their leaders,

167

or are they themselves transformed and less dependent on leadership? If the latter alternative, of a more resilient organization, is closer to the truth, then killing the leaders of the adversary obviously will be less effective, and killing their leaders may not be a way to stop the transformation of their organizations—on the contrary, it might hasten it. The fate of Hamas is an illustration. Numerous successive top leaders of Hamas have been killed, but the organization has so far been able to replace them or in other ways made itself less vulnerable to the loss of leaders. The age-old offensive doctrine of the importance of killing leaders is at least ripe for renewed analysis, and maybe it is time for revision. The defensive doctrine of how to protect your leaders from being killed may also be ripe for revision. There are interesting modern alternatives to bunkers and bodyguards, such as network-centric organizations and the introduction of team- and co-leadership.

Interpreting the Shooting Down of Yamamoto Using Leavitt's Diamond

Imperial Japan's most revered military leader, Admiral Isoroku Yamamoto, was killed on April 18, 1943. His plane was shot down during an inspection tour of the Solomon Islands, east of New Guinea. The twin-engine bomber carrying Yamamoto was escorted by six Mitsubishi A6M Zeros. They had no chance of defeating an ambush by 16 Lockheed P-38 Lightnings (the only U.S. fighter capable of flying 700 km "on the deck" to make the interception). The interception was made possible by American codebreaking, which had obtained Yamamoto's itinerary for the inspection tour. That hot piece of information went all the way up the chain of command to President Roosevelt, who gave his go-ahead order to Navy Secretary Knox, Fleet Admiral Nimitz, and Admiral Halsey, and down the chain of command to fighter squadron 339 at Guadalcanal. The squadron did excellent planning and delivered a surprise attack near Bougainville Island. Because it was vital to keep the American codebreaking secret, a deceptive story had to be invented and spread through the media about Yamamoto having been observed by some pro-American native people at Rabaul Island.[1]

---

[1] Admiral Yamamoto was under hard pressure from Imperial Headquarters, and not least from Emperor Hirohito, to compensate for the loss of Guadalcanal by an offensive in the Northern Solomon Islands. See H. Bix, "The Ordeal of Supreme Command," in *Hirohito and the Making of Modern*

If we use Leavitt's diamond[2] as a frame of reference for analyzing the killing of Yamamoto, it is obvious that the right kind of interplay among people, technology, organization, and process was critical to the outcome. Without people capable of codebreaking, there would have been no attack whatsoever. With a lesser fighter than the P-38, or fewer fighters, Yamamoto might have escaped. If the American chain of command from the Commander in Chief down to the hierarchy within the squadron had been only somewhat slower, the opportunity for killing Yamamoto would have been lost. In a chain of events, the weakest link tends to define the outcome. There was no weak link in the chain of events ending with the crash of Yamamoto's bomber.

History is filled with failed attempts, such as those to kill Hitler. The cost of such failures is not only that the "target" survives. In the case of Hitler, his conviction that he was chosen by destiny to rule (without listening to advisers) was very much strengthened after each failed attempt, in particular the one by Count von Stauffenberg, on July 20, 1944. But what are the benefits of success?

The consequences of success in killing Yamamoto are still debated. The importance of his death for the American public was in delivering a boost of morale and delivering part, but only part, of the revenge for Pearl Harbor. Now the highest commander of that infamous attack had been punished. There is also agreement among historians that the effects on Japanese morale were devastating. The news of Yamamoto's death was kept secret in Japan for month, until May 21. On June 3, he was honored with one of the most-attended state funerals in Japanese

---

Japan (New York: HarperCollins, 2001). Bix' Pulitzer Prize–awarded book presents a new and more militant portrait of the emperor than the traditional one.

[2] Harold Leavitt (1922–2007) was one of the most interesting proponents of the sociotechnical school of thought, with a PhD from MIT and being a professor at Stanford Business School for many years. The common denominators of the sociotechnical school are the holistic approach and the belief in organizational choice in opposition to technological determinism. The holism is often not broader than the two factors, the social system and the technological system, however. Leavitt has four factors—tasks, structure, technology, and people—in his famous "diamond," first presented in *Managerial Psychology* (1964). I use the modification by Garstka (2008) and call the factors process, people, technology, and organization. See also essay 2.

history.[3] His death was seen as a very bad omen and shook the nation's collective belief in final victory. In the Japanese military hierarchy, no one could replace him intellectually. His standing in Japanese society has been compared to that of Marshall, Nimitz, and MacArthur combined.

On the other hand, what was the value of his brilliance after the tide had turned in the war in the Pacific? His leadership had not saved the Japanese attack fleet from defeat at Midway in June 1942. Are time and timing general aspects of "process"? If not, Leavitt's diamond is not up to the mark of explaining all the effects of this kill; if they are part of process, there is a pretty good fit between model and reality for this case.

Four Murdered American Presidents and the Use of Leavitt's Diamond as a Frame of Reference

Four American Presidents have been assassinated while in office: Abraham Lincoln (1865), James Garfield (1881), William McKinley (1901), and John F. Kennedy (1963). Which factors decide the importance of these killings? Can we use Leavitt's diamond of process, people, technology, and organization to gain a better understanding?

The organizational context is an important key in analyzing the effects of the killings of the presidents. In the United States it is no enigma who will become the successor on the death of the president. The founding fathers determined, and later Amendments clarify, who is next in the presidential line of succession, the first person being the vice president and the second the speaker of the House of Representatives.[4] This is, of course, an advantage over systems in which the succession is not predetermined. After the murder of Caesar, for instance, civil war raged for 17 years. The murderers believed they were saving the republic by stabbing Caesar. Instead, they helped bring imperial pretenders to power (via triumvirs defeating each other one after the other). Starting with Augustus in 27 BC, the Roman Empire was ruled by emperors for five centuries.

---

[3] The funeral was filmed; part of it can be seen in the famous BBC series from the 1970s, "The World at War."

[4] To be effective, it is important that the line of succession is well-known. It was rather shocking for the American media when Secretary of State Alexander Haig declared immediately after the failed attempt to kill Ronald Reagan in 1981 that he, Haig, was in charge.

Calling attention to the unintended consequences of murder, King Herod's order to kill all male children in Bethlehem failed to achieve his objective to kill the newborn "king of the Jews." Three decades later, the execution of Christ was not the end of Christianity, but was instead its birth as a world religion. The long trial of the 19-year-old Joan of Arc ended with her burning on May 30, 1431. Her execution did not ensure the victory of England and Burgundy in the Hundred Years' War (1337–1453). On the contrary, it kindled French nationalism and changed the character of the war from one marked by dynastic turmoil about who was the true heir to the throne of France into one of national identity. The end of the war was also the end of British rule on the French mainland; the only remnants today of William the Conqueror's Normandy possessions are the Channel Isles of Jersey and Guernsey.

Killing is, of course, about people. What kind of person are you killing? The caliber of the one killed is thought to correlate closely with the effects of the killing, but killing leaders is using a double-edged sword, metaphorically speaking. What about the quality of the successor? The advantage of the American presidential line of succession is swift and orderly succession; for instance, within minutes after the death of Kennedy. The risk and drawback of the system is that the presidential qualifications of the vice president are often neglected when the presidential candidates are choosing a running mate for the election campaign. Andrew Johnson became president after the assassination of Abraham Lincoln. He was the only southern senator who remained loyal to the Union during the American Civil War. Apart from that merit in the election of 1864, however, he had few credentials, at least on a presidential level and is generally considered a failure as president. He is ranked 37th in a list of 40 ranked U.S. presidents.[5] When he was impeached, the 10th article of the impeachment rather tellingly asserts, "Andrew Johnson has brought the high office of President of the United States into contempt, ridicule and disgrace, to the great scandal of all citizens."[6]

---

[5] J. Taranto, ed. *Presidential Leadership* (New York: Free Press, 2004). The ratings in this book are based on evaluations made by experts on presidential leadership. There are numerous other ranking lists on this very popular subject. The most striking differences between experts and public opinion concern 19th-century presidents, many of whom have been forgotten by the general public.

[6] Cited from Taranto, *Presidential Leadership*, 92.

James Garfield was only president for a few months, so he is usually not ranked at all. His successor, Chester Arthur, is thought of as being below average. William McKinley was succeeded by Theodore Roosevelt, who outshone McKinley and is considered to be one of the 10 best Presidents ever. However, McKinley is held in high esteem among experts as the creator of the modern presidency and for presiding over a vast extension of U.S. influence from Puerto Rico and Cuba to Guam and the Philippines after the Spanish-American War.[7] John F. Kennedy is a legend. His successor Lyndon Johnson might have been one, based only on domestic politics, but that legacy is much overshadowed by his controversial role in and support for the Vietnam War.

The process is also of grave importance—more precisely, when and where in the process. From a process perspective, the killings of James Garfield and William McKinley were not very fateful, whereas the killing of Kennedy, on the contrary, ended a very promising presidency that lasted only a thousand days.[8] Lincoln was killed on April 14, 1865, with 3 years left of his second term and only 5 days after Lee's surrender at Appomattox. What triggered his assassin, John Booth, was a speech Lincoln had delivered 3 days earlier in favor of voting rights for blacks. Booth succeeded in killing not only the president but also the process of reconciliation that had just begun, as well as numerous other promising initiatives by Lincoln. The negative effects of Booth's intervention into history are generally estimated as enormous. It is doubtful if the concept of "process" is broad enough to mirror all these effects, and if so, Leavitt's diamond must be judged as too simplistic in interpreting these historical events.

Anarchist Terrorism

William McKinley was killed by an anarchist. Anarchism means, in Greek, "without rulers." Combined with another anarchist idea,

---

[7] To cite just one of many experts on presidential leadership sharing this view, R. Dallek, *To Lead a Nation: The Presidency in the Twentieth Century* (New York: Barnes and Noble, 2004). In particular the first lecture: *The Rise of the Modern Presidency.*

[8] Referring to the legend of the Celtic King Arthur, Jacqueline Kennedy called the John F. Kennedy presidency "Camelot," a characterization still in use. An indication of his legacy is the fact that "John F. Kennedy" is still, in 2009, the biggest site on Wikipedia, in all categories.

"propaganda of the deed,"[9] the conclusion might seem, consequentially, that killing rulers will contribute to a world without rulers, or at least to a world where rulers are less autocratic. Anarchist terrorism was practiced for at least 40 years. Tsar Alexander II was assassinated by an exploding bomb in 1881 after many earlier failed attempts. The liberal Alexander II, who among many other reforms abolished serfdom in Russia, was succeeded by his very autocratic son, Alexander III. The killing of Alexander II was, in other words, no proof of the validity of the anarchist "kill the rulers" theorem. French Prime Minister Carnot was assassinated in 1894. Spanish Prime Minister Canova was assassinated in 1897. Italian King Umberto I was assassinated in 1900, and Russian Prime Minister Stolypin was killed in 1911. This list could be made much longer by adding lesser "rulers;" for instance, chief executive officers in industry killed by anarchists, and could be made much, much, longer by the many failed assassination attempts. The successful killings never resulted in a country or an organization "without rulers." In that sense the anarchists' view of the world was proven utterly wrong. Invariably, their deeds resulted in a faster turnover of rulers, however, and their killings had various unintended consequences.

The assassination of Archduke Franz Ferdinand and Countess Sophie in Sarajevo in Bosnia and Herzegovina on June 26, 1914, is maybe the most striking example of how hard it is to anticipate the outcome of a killing.[10] The young royal couple was fired on by an even younger Serbian nationalist and anarchist, Gavrilo Princip. It is a matter of debate as to what extent this killing furthered Serbian interests. It certainly did not leave Austria-Hungary without a ruler, as Emperor Franz Joseph was still in power, or without heirs to the throne. What is certain is that Princip's mortal shots in Sarajevo started an extremely complicated chain reaction leading to the Great War. In that war, more than 4 years long, some 60 million men were called up to military service, and some 20 million were killed. Three empires—the Russian, the German, and the Austrian—collapsed during and as a result of the Great War, not to mention countless other effects, among which can be counted World War II. Perversely, given Princip's purpose, the Great War hit Serbia especially hard because of famine and an outbreak of

---

[9] Many are referred to as having formulated this principle, one of the earliest and most influential being Mikhail Bakunin (1814–1876).

[10] B. Tuchman, *The Guns of August* (New York: Dell, 1963 [1962]).

typhus, which killed at least half a million civilians out of a population of 4.5 million. After that war, Serbia was enlarged and the people of Bosnia-Herzegovina experienced the mixed blessing of exchanging Austrian rule and dominance for Serbian control. We have recently witnessed a civil war in former Yugoslavia focused on liberation from Serbian dominance.

It is often argued that the Great War would have come regardless of what Princip did or did not do. He struck a match, but he cannot be held responsible for the enormous accumulation of combustible material in Europe in the summer of 1914. One can say that Princip decided the timing. Who knows what a few more months or years of peace would have achieved. The first (1905–06) and second (1911) Moroccan crises were overcome and did not, as so many feared, lead to war. The Great War might have been postponed or might have turned into quite another war had not Princip fired those shots.[11] Some even argue that it might have been avoided by negotiations similar to those ending the Moroccan crises and some similar encounters in the "Belle Époque." It is asking a lot of Leavitt's diamond to expect it to be a valid frame of reference for analyzing the effects of the shots in Sarajevo. The most decisive example in our evaluation of Leavitt's diamond is these shots, however, and we will return to them at the end of this essay.

Anarchism is not dead. There are many different kinds of anarchism, and the variation is striking. The term anarchism is not very telling. The militant form of anarchism, and in particular the terrorist form, has from time to time reemerged, however, as happened during the Spanish Civil War and in Europe in the 1970s and 1980s. The red brigades, the BR ("Brigate Rosse") in Italy and the RAF ("Rote Armee Fraktion") in Germany, had the killing of "rulers," mainly in business but also in politics, on their agenda. In both Germany and Italy, these organizations and their members were called anarchistic terrorists by the authorities when pursued by the police and when arrested and convicted, but it might be fairer to characterize them as of rather mixed ideological origins. For instance, they were obviously inspired by the urban guerrillas of Uruguay—the Tupamaros—as well as by many different communist groupings and fractions.

---

[11] "If-not history" is a genre of its own. See J. Langdon, *July 1914. The Long Debate 1918–1990* (New York: Berg, 1991) for many examples of that kind of analysis.

Well-known German bankers and industrialists were killed by the RAF in 1977. The Italian PM Aldo Moro was kidnapped in 1978 and was later killed by the BR. In 1975, there was an early attempt by the RAF to occupy the German embassy in Stockholm. In most respects it was a failure, but the occupants killed the German military and trade attachés. The RAF in particular tried, mostly in vain, to destroy American and NATO installations in Germany. One such RAF attack in June 25, 1979, targeted the Supreme Allied Commander Europe of that time, Alexander Haig; the guard car following him suffered heavy damage, but Haig was unharmed. The RAF was in a very obvious way anti-American and was heavily supported by the Deutsche Demokratische Republik, a fact not well known in the West in the 1970s and 1980s.[12]

Some Sniper History

Three presidents were killed by point-blank fire. Kennedy was killed at long range by a sniper, if we believe the conclusions of the Warren Commission. This seemingly minor change in technology from close- to long-range fire has had far-reaching effects on the political culture in many countries, making high standards of security so much harder and costlier to achieve.

Snipers and sniper technology have a long history of their own. The theoretical point of departure is the understanding, or shall we say belief, that killing leaders might change the outcome of a battle. During the Napoleonic wars, at least one French Navy captain, Jean Lucas, thought snipers had the potential of being decisive.[13] He identified that the weakest point in the British Navy was its strong dependence on a well-functioning hierarchy on commanding captains in particular. During the battle of Trafalgar in November 1805, he was given the opportunity to test his ideas. His ship, *Le Redoutable*, was one of those in close fight with Nelson's flagship HMS *Victory*. A bullet from a sniper high up in the mizzen-mast of *Redoutable* passed through Nelson's spine, ending his life within a few minutes. That was a

---

[12] The literature on the RAF is voluminous. One of the more inclusive works analyzing the RAF from various perspectives, even telling the story of the fight against them, is the one edited by W. Kraushaar (ed.), *Die RAF und der linke Terrorismus* (Hamburg: HIS, 2006).

[13] Page 76 and onward in J. Keegan, *The Price of Admiralty. The Evolution of Naval Warfare* (London: Penguin Books, 1988).

tremendous loss, killing arguably the greatest sea captain ever, but the battle was already won by the British at the time of his killing. The victory at Trafalgar changed world history and lay to rest Napoleon's plans of invading the British Isles. It even meant the beginning of the end of Napoleonic rule over continental Europe. Once more we see the importance of process. Had Nelson been killed before he had had his planning meeting with his captains, introducing his new bold and innovative battle plan, the killing might have been decisive. Instead, the death of a hero was a great inspiration for at least a century of British Rule the Waves policy.[14]

Snipers are nowadays a normal component of all armed forces. They seldom get world leaders in sight but are used for killing people of lesser importance. That makes quantity more important. The Finnish sharpshooter Simo Häyhä[15] killed more than 500 Russian officers and soldiers during 3 months of fighting (November 30, 1939–March 13, 1940),[16] the so-called Winter War, including more than 30 Russian sharpshooters designated to kill him. On March 6, Häyhä was hit by an explosive bullet in his face but survived the war, although disfigured.

The potential effectiveness of selective killings had been demonstrated already during the invasion of Poland in early September 1939. German agents shot a substantial number of Polish pilots in their homes before they were able to mobilize. That was a severe blow to the Polish Air Force, as pilots are even harder to replace than officers. For example, their replacements might have had fewer than 100 flying hours and were thus easy prey in dogfights against more experienced adversaries.

The Russian military learned the lessons taught to them by Häyhä—not the least of which was the sniper's importance for psychological warfare, in this case the constant threat of an unexpected bullet from some sniper far away. Häyhä was widely called the "White Death." The Red Army used many sharpshooters during World War II, with German noncommissioned officers as their prime target; for instance, during the siege of Stalingrad. Some female sharpshooters became great heroines in the Soviet Union, such as Lyudmila Pavlichenko, who after 309

---

[14] A. Herman, *To Rule the Waves: How the British Navy Shaped the Modern World* (New York: HarperCollins, 2004).

[15] T. Saarelainen, *The Sniper: Simo Häyhä* (Helsinki: Apali Oy, 2008).

[16] Some, for instance Wikipedia, claim this is an unsurpassed record.

confirmed kills became a sniper instructor and was commemorated on stamps during and after the war.

In Soviet military doctrine, the killing of leaders was central and was applied brutally. Executioners were treated as valid alternatives to snipers, with complete disregard for international law. The history of the Gulag archipelago is one of killings—mostly slow killings—of enemies of the state. Many of the secrets of that world of prisons and labor camps will most likely never be unveiled, as denials and disinformation were characteristic of the Soviet regime. For a long time, the Soviets blamed the Nazis for the "Katyn massacre," which to Western eyes seemed to fit with all the other atrocities—crimes against humanity and genocide—that the Nazis committed in Poland during the years of the Holocaust. Compared with the seven million who were exterminated in the concentration camps, some thousands of killed officers was only a detail. Everything is relative, especially in comparison to the worst atrocities in human history. It was also well known that the Schutzstaffel, or SS, and Gestapo gave priority to killing political commissars and members of the Communist party, thus making it plausible that they would have killed imprisoned officers. However, seldom, if ever, has the doctrine of killing the leadership been applied on the scale of Katyn. Twenty thousand Polish prisoners of war, mostly officers, were killed, one at a time, by a shot through the back of the head. The killings went on day after day during April and May 1940 in the Katyn forest and some similar forests, with the aim of eliminating the Polish officer corps. Those killings dealt a severe blow to the whole of the Polish intelligentsia as well, as most Polish men with a university degree—engineers, lawyers, physicians, and so forth—were officers in the reserve. Many of them were quite recently mobilized and their units, in retreat, had been driven by the advancing German divisions toward the eastern part of Poland in the belief that that part of the country was safe.[17] Beria, the head of the Soviet secret police, came up with the idea for this massacre, and Stalin gave the order. It remained unknown, however, until the mid-1990s, when

---

[17] An ambitious interpretation of that massacre can be seen in a recent film by A. Wajda, "Katyń" (2007). The film has already received a dozen awards and an Oscar nomination. Apart from giving an account of the massacre, the film also portrays what happened to those Poles who opposed the Soviet falsification of what had happened.

documents showing these orders and signatures were released by direct command from Boris Yeltsin,[18] thereby clarifying the quest for guilt.

Stalin was, as we know, familiar with mass killings.[19] For him, as well as for many other leading Bolsheviks, the French revolution was a benchmark. Stalin in particular feared that the Soviet revolution might end in "Bonapartism,"[20] meaning that a new Napoleon would come to power. His way of dealing with that threat was paranoid: Kill all Russian officers with the slightest resemblance to Napoleon. The officers bearing that resemblance totaled more than 10,000. Although Marshal Tuchatjevskij was possibly as bright and innovative as Napoleon, any resemblance between Napoleon and most of the other executed officers was greatly stretched. For some, guilt warranting death was established by the mere knowledge of a foreign language. For others, it was established by having met foreign officers—for instance, during those years in the 1920s when the Weimar Reichswehr was allowed secret access to Russian training grounds. At the end of the 1930s, such officers were often high ranking but were still executed without mercy.

Many see a strong correlation between the purge of the progressive Soviet military leadership and the disastrous lack of Soviet military leadership during the second half of 1941. During 5 months, a staggering 4 million Soviet soldiers were killed or taken prisoner, and the German invaders reached the outskirts of Moscow. The purge of the Soviet officer corps in the 1930s was a field experiment—unintended and very costly—in all meanings of the word, proving the importance of competent leaders. Hopefully, that lesson has been learned in more countries than Russia. During World War II, younger Soviet officers had to improve their capacity to command larger units very swiftly, and mostly under very demanding conditions. The failure rate was high. Quantitative superiority—two to one in manpower reserve—helped save the Soviet Union, but they used a lot of that reserve.

---

[18] B. Fischer, "The Katyn Controversy. Stalin's Killing Fields." (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005).

[19] S. Montefiore, *Stalin. The Court of the Red Tsar* (New York: Alfred Knopf, 2004).

[20] Stalin borrowed his analysis of this phenomenon from Karl Marx. K. Marx, *The Eighteenth Brumaire of Louis Bonaparte* (Moscow: Progress, 1937 [1852]).

History contains many infamous uses of sharpshooters when sheer terror and not the targeting of leaders was the real aim. During the Serbian siege of Sarajevo, the Serbian snipers maintained "Sniper Alley," 1992–1996, 80 years after the shots in Sarajevo. The Serbian snipers terrorized the inhabitants of Sarajevo for 4 years, wounding more than a thousand and killing a few hundred—among them more than 60 children.[21]

In conclusion, the history of snipers and sharp shooters started with very important leaders, such as Nelson, being the target. For two centuries, quantity has gained in importance, with the elimination of all leaders of an organization, as in the Katyn massacre, as the other ideological extreme.

Suicide Terrorism

When the killer is suicidal, the rules of the game change. Applying the Leavitt diamond, we can start with people. The deterrent effect of the death penalty on a potential killer is a controversial one, but in suicidal attacks the killer has already dismissed it. Threatening him (or her, now) with a severe punishment is of no use, and thus a new kind of deterrent is required. You have to come up with some new deterrent. You have, for instance, to find and catch those backing the aggressor—you have to target the organization behind the actor. The whole process is different, too; for example, an exit strategy for the aggressor is no longer necessary. This new option improves the odds for the killer, making him or her much more effective. The use of technology is changing as well. A bomb load might be delivered by a low-tech but intelligent targeting device: an adaptive human being with situational awareness.

Suicidal killings had already been introduced during World War II, when the Japanese high command became desperate because of the very obvious turn of the tide of the war in the Pacific. The kamikaze pilots were usually not very well trained; the experienced Japanese pilots, who were also the more qualified instructors, had already died. The Kamikaze pilots were trained to dive bomb all the way into the target, thus eliminating the need for calculating a separate bomb

---

[21] Simms gives a close account of the siege in his eighth chapter, "The Reckoning," which includes the story of the final breakthrough under the leadership of Rupert Smith. B. Simms, *Unfinest Hour. Britain and the Destruction of Bosnia* (London: Allen Lane, 2001).

parabola. The principal target for kamikaze pilots was American capital ships. There was no specific doctrine on prioritizing leadership as a target, but since it was thought to be easier to attack the biggest ships, hitting command and control functions was often a side effect.

Suicidal terrorism was reintroduced in the late 1960s with the hijacking of airliners. One of the earliest attacks was a Popular Front for the Liberation of Palestine hijacking on July 23, 1968, of an El Al airliner bound for Tel Aviv from Rome, which was then forced to fly to Algiers instead. In the 1970s, 1980s, and 1990s, there was a rather steady number of aircraft hijackings. The main defensive strategy has been, as we all know, stricter passenger checks and surveillance at the gates, but they have not proven to be strict enough. The worst hijacking ever was the September 11, 2001, terrorist attacks against the World Trade Center and the Pentagon, in which passenger airliners were used as kamikaze planes.

By and large, terrorists, have shifted emphasis away from killing leaders. The 1983 Beirut barracks bombing, which used a truck filled with explosives and resulted in 241 deaths, targeted ordinary marines, not leaders. The same day, the French Foreign Legion was attacked in a similar way, and 58 people were killed. The terrorists of today seem to prefer killing innocent people—the more the better. Explosive devices effectuate this goal, and because they are easily concealed beneath clothing, gain the advantage of surprise. Depending on the size of the bomb and the place where it is detonated, the effects might be far-reaching. Blowing up people commuting on buses and trains is now a common act of terrorism. In an analysis of 600 acts of suicidal terrorism from December 1981 to July 2005, by Ami Pedahzur,[22] some patterns become very obvious, such as hitting places where people gather—shops, malls, markets, mosques, churches, stations, airports, trains, buses, restaurants, nightclubs, hotels, and even a few hospitals.

One possible explanation for this fundamental difference between anarchist terrorism and suicidal terrorism—targeting leaders versus targeting common people—is that at least two lessons have been learned. First, it is hard to succeed in killing leaders, because they are nowadays normally well protected by bodyguards and sophisticated technology. Second, if one succeeds in killing a leader, a new one will simply replace the killed one, and the second leader is often tougher against terrorists than the first one, as was the case when Tsar

---

[22] Appendix in A. Pedahzur, *Suicide Terrorism* (Cambridge: Polity, 2005).

Alexander III succeeded Alexander II. Killing does not create a "world without rulers," as the naive vision of the anarchists promised. On the contrary, it often brings tougher leaders to power.

Trying to kill ordinary people performing the most common of activities is much more likely to lead to actual killings, as these people are not as well protected as top leaders and never will be. It is impossible to create such a fool-proof, terrorist-free society. The question remains, What do the terrorists believe they are achieving by killing ordinary people? It is certainly not the way to win the hearts and minds of the survivors—the friends and relatives of the killed ones. What the killings do achieve is terror. The terrorists might think that their terror in the long run will lead to the breakdown of the existing society, at which point their organization will be ready to take command. This rests on the hypothesis that the terrorists have a shared vision, which is so far still just a hypothesis.

In Iraq, the frequency of suicide attacks reached unprecedented levels after the initial success of the invasion. The attacks in Iraq follow a somewhat different pattern from suicidal terrorism in other countries. An early suicide attack took place on August 19, 2003, in which a truck filled with explosives was driven into U.N. Headquarters. In the blast, some 20 people were killed, among them the U.N. special envoy to Iraq, Sergio de Mello, and more than a hundred people were wounded.

Many of the thousands of attacks that have followed have targeted coalition troops, and American soldiers at checkpoints in particular. They have also prioritized Iraqi police stations and queues of police applicants. A number of the attacks have also targeted rival religious groups when they are gathering at various religious sites. By and large, the attacks have been more warlike than the suicidal attacks in, for instance, Israel.[23]

Killed Leadership and Organizational Resilience

Osama Bin Laden still has not been caught, despite a reward of up to US$25 million. He is known under at least 10 aliases and is believed to be hiding in the mountainous region bordering Afghanistan and

---

[23] An early analysis discovering this pattern is Thomas X. Hammes, *The Sling and The Stone. On War in the 21st Century* (St. Paul, MN: Zenith, 2004). In the vast literature on the war and insurgency in Iraq, Thomas Ricks gives an overview of the first three years in *Fiasco. The American Military Adventure in Iraq* (London: Penguin Books, 2006).

Pakistan. We do not know for sure why he has not been caught as, for instance, Saddam Hussein was. The terrain mentioned is well-suited for hiding. He might be a skillful fugitive, or he might be dead—we do not know. My bet is that he is well protected a very loyal "band of brothers" and that the Al Qaeda organization will function even if he is killed.

The "brotherhood" principle is not new. It has been practiced by some of the greatest leaders of the past.[24] Horatio Nelson, for example, had a collegiate style of leadership toward his closest subordinates, the captains of his fleet. They were always invited to participate in his planning before major battles—a practice started before the Battle of the Nile, August 1, 1798, and made legendary after Trafalgar.[25] Nelson knew his Shakespeare and brought his favorite play, Henry V, along on his voyages. He used the quote from the playwright's famous St. Crispin's Day Speech to characterize what he wanted from his captains—tactical independence and bold action: "We few, we happy few, we band of brothers."[26] The captains knew their commander's intent and could and would go on trying to realize it. Earlier in this essay we introduced Jean Lucas, whose snipers managed to kill Nelson at Trafalgar, but Lucas was in the end disappointed—killing Vice Admiral Nelson did not prevent the defeat of the French-Spanish armada. In later battles, the most inspiring British signal became "Remember Nelson."

A model organization for many of today's Muslim networks is the Egyptian Muslim Brotherhood, founded in the 1920s. That brotherhood is used to working underground and clandestinely, having been persecuted by the authorities. Now and then, their leaders have been put in jail or killed. Organizations like Hezbollah, Hamas, and Al Qaeda share the same fate: Many of their leaders have been killed. Israeli Defence Forces and Mossad, for example, have pinpointed the leadership of Hamas. In the spring of 2004, they killed both the top

---

[24] This is not implying that Osama Bin Laden should be ranked as a great leader—he is far from that—but only that he is using the famous brotherhood formula.

[25] R. Knight, *The Pursuit of Victory. The Life and Achievement of Horatio Nelson* (New York: Basic Books, 2005).

[26] Shakespeare is imagining Henry V giving this inspired speech before the Battle of Agincourt on St. Crispin's Day, October 25, 1415. Agincourt is the greatest English victory during the Hundred Years War and is most famous for the role played by English longbow archers against French knights.

leader Yassin and his successor Al-Rantisi within weeks. These organizations are often called networks, most commonly Al Qaeda. Do we know that they are networks? I have my doubts. What we do know is that they have survived the loss of many of their leaders, but the same has been true of most undercover organizations in history, including spy organizations, forbidden parties, partisan organizations, and resistance movements.

The defensive trick used by these organizations is simple and age-old: keep the organizational chart secret, in particular from the very members of the organization. Then they cannot reveal it, not even under torture. Once one can get the name of a contact from each cell, one can painstakingly map the organization. The French did that in Algiers in the late 1950s, uncovering National Liberation Front leadership, but certainly violating international law in the process. The French attempt seemed successful for some years in the middle of the 1950s,[27] but then the rebellion against French rule was resurrected, more forcefully than before, and Algeria gained its independence. The Algerian example is often referred to nowadays as proving that insurgencies can be crushed militarily. That argument misses the point that the Algerian insurgency succeeded politically only 2 years after the alleged military defeat.[28]

However, if killing the leader is not enough, maybe killing the whole band of brothers is. That strategy is being tried right now by the Russians in Chechnya. It was also tried during the 1950s by the British in Malaya. The British victory over the communist rebellion in Malaya, a rebellion called the Malayan Emergency, a euphemism typical of the 1950s, is certainly one of very few examples of a victory over a rebellion. But looked at more closely, the famous British "winning the hearts and minds" campaign led by Field Marshal Gerald Templar at that time seems rather similar to the old imperial *divide et impera* principle. It was not that hard to isolate the communist insurgents in Malaya, as they were Chinese, and the importance of the ethnic issue and the ethnic tensions was proven a few years later, when the Malayan

---

[27] In the masterly Italian film "Battle of Algiers," by Pontecorvo (1966), the systematic elimination of the secret hierarchy of FLN by the French paratroopers under the leadership of General Massu is given a detailed account.

[28] In David Galula's (1964) famous analysis of an insurgency, it is claimed to be 80% political, 20% military. David Galula himself was an extraordinarily successful field commander in Algeria during the French rule.

Federation was broken into two parties—the mostly Chinese Singapore seceded from the Federation in 1965, making Malaysia Malayan.[29]

More or less indiscriminate killing is against international law. Using such an approach means you are losing the moral high ground. An alternative to indiscriminate killing was practiced early on in Iraq by the Americans in 2003 and 2004, exemplified in the distribution of a deck of cards of "most wanted" ex-leaders. The cards did not sentence the Hussein supporters to death but only proclaimed that they were wanted by the Americans. Some, like the notorious brothers Uday and Qusay Hussein, were killed when they refused detention. Others had to face prosecution and court proceedings.

Underground organizations have to adapt to getting many in their leadership killed. If they do not succeed with that adaptation, they will most likely perish. However, according to the most recent studies of terror organizations, they are adapting, and quite successfully.[30] Looked at more closely, Sageman's thesis of leaderless organizations is a misnomer. They are not leaderless but, rather, good at succession and using what military experts would call *Auftragstaktik* (far-reaching delegation)—their organizations have become resilient.

Amid Pedahzur[31] concludes his analysis of suicidal terrorism with a pessimistic evaluation of the military options for eliminating the leadership of these organizations in the long run. Some other strategy, beyond a lone military one, is needed. Terrorism, even suicide terrorism, must be dealt with in a more comprehensive way. This much is evident at the present stage: the strategic alternative in demand will contain a number of civilian elements and endeavors.

---

[29] John Nagl's much acclaimed book, *Learning to Eat Soup with a Knife*: *Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: University of Chicago Press, 2002), with its reverence for Lawrence of Arabia, underestimates the ethnic issue, in my view. I also think it overstates the lessons to be learned from a victory over 6,000 rebels in comparison to the civil war in Vietnam, where the some hundred times larger communist rebellion was supported by the well-organized North Vietnam and its regular army.

[30] I am specifically thinking of Marc Sageman's latest book, *Leaderless Jihad*: *Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008).

[31] Pedahzur, *Suicide Terrorism*.

Summary

Snipers and sharpshooters are still intact elements of modern armies, and suicide terrorism is far from wiped out. On the contrary, an increasing number of organizations are using it. Judging from the many bombings of recent years, the terrorists manage to find new recruits of willing assassins. Lone and mad murderers also must be added to this list. In short, killing leaders and leadership will go on in the years to come.

The mindset of the assassins is often simplistic. The anarchists thought that killing leaders might in the end bring about a "leaderless world."[32] The suicidal terrorists of today have, in comparison with anarchists, more limited aspirations, but still far-reaching and often dramatic ones: the independence of Chechnya, the elimination of the state of Israel, an American military withdrawal from Iraq, or a triumphant Taliban movement.

The Leavitt's diamond is a model that might help us avoid simplistic analysis. It is a kind of checklist reminding us of the importance of process, people, technology, and organization. It is an important development compared with, for instance, "technological determinism," which was much in vogue before Leavitt. Emphasizing the importance of four factors widens the applicability of his model in comparison with sociotechnical analysis—an analysis identifying only two factors: technology and the social system. The interplay of the factors in the diamond model might define the window of opportunity.

We began by using the shooting down of Yamamoto as an illustration of skillful planning and execution considering all four factors (process, people, technology, and organization), but when we added examples of how and why leaders have been killed, the Yamamoto example got a new meaning as an extraordinary exception to the rule. In general, the most striking outcome of assassinations is the many unintended and unforeseen consequences. The assassins have not had enough foresight, but in most cases they have been in very good company, as unfortunately, no one else had foresight either. Princip was certainly not able to foresee the many processes set in motion by his shots in Sarajevo. Few—very few—seemed to be able to foresee these processes, and no one was able to change or stop them. Leavitt's model is a model fit for middle-range processes, not grand

---

[32] The original meaning of the word "anarchism."

history. It is, however, hard to know when the first ends and the second begins.

Confronted by a case of a killed leader—or worse, killed leadership—it might be useful to start analysis using Leavitt's diamond. One advantage of such an exercise is that we do not forget the importance of organization and process. In an era of asymmetrical warfare, no one can afford forgetting the importance of these aspects. Some terror organizations seem to be more transformed organizationally than the counterinsurgency organizations supposedly teaching them a lesson they will never forget. Leavitt's model can be used as a reminder of the challenges of transforming process, people, technology, and organization and managing a skillful interplay of these factors, but by and large, applying Leavitt's model is only a start. A four-factor model is incapable of revealing a reality that is infinitely more complicated. What we experience as unintended consequences of a leader being killed might be caused by a factor x or n-factors that are not part of Leavitt's model.

References

Bix, H. (2001). *Hirohito and the Making of Modern Japan*. New York: Perennial.

Coughlin, J. et al. (2005). *Shooter. The Autobiography of the Top-Ranked Marine Sniper*. New York: St. Martin's Press.

Dallek, R. (2004). *To Lead a Nation*. New York: Barnes & Noble Audio.

Fischer, B. (2005). "The Katyn Controversy. Stalin's Killing Fields." *Studies in Intelligence*. Washington, DC:

Galula, D. (1964). *Counterinsurgency: Theory and Practice*. New York: Praeger.

Garstka, J. (2009). *A Conceptual Framework for Transformation*. Washington, DC: Pentagon.

Gunaratna, R. *Inside Al Qaeda. Global Network of Terror*. London: Hurst.

Hammes, T. (2004). *The Sling and The Stone. On War in the 21st Century*. St. Paul, MN: Zenith Press.

Herman, A. (2004). *How the British Navy Shaped the Modern World. To Rule the Waves*. London: Hodder.

Kean, T. & Hamilton, L. (2004). *9/11 Report*. New York: St. Martin's Paperbacks.

Keegan, J. (1988). *The Price of Admiralty. The Evolution of Naval Warfare*. London: Penguin Books.

Knight, R. (2005). *The Pursuit of Victory. The Life and Achievement of Horatio Nelson*. New York: Basic Books.

Kraushaar, W., ed. (2006). *Die RAF und der linke Terrorismus.* Hamburg: HIS.

Langdon, J. (1991). *1914. The Long Debate 1918-1990.* New York: St. Martin's Press.

Leavitt, H. (1964). *Managerial Psychology.* Chicago: University of Chicago Press.

Marx, K.. (1937/1852). *The Eighteenth Brumaire of Louis Bonaparte.* Moscow: Progress.

Montefiore, S. (2004). *Stalin. The Court of the Red Tsar.* New York: Alfred Knopf.

Nagl, J. (2002). *Learning to Eat Soup With a Knife. Counterinsurgency Lessons from Malaya and Vietnam*. Chicago: University of Chicago Press.

Pedahzur, A. (2005). *Suicide Terrorism.* Cambridge, MA: Polity.

Ricks, T. (2006). *Fiasco. The American Military Adventure in Iraq*. London: Penguin Books.

Saarelainen, T. (2008). *The Sniper*. Helsinki: Apali Oy.

Sageman, M. (2008). *Leaderless Jihad. Terror Networks in the Twenty-First Century.* Philadelphia: University of Pennsylvania Press.

Sageman, M. (2004). *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press.

Simms, B. (2001). *Unfinest Hour. Britain and the Destruction of Bosnia*. London: Allen Lane.

Shapiro, R. et al., eds. (2000). *Presidential Power.* New York: Columbia University Press.

Taranto, J., ed. (2004). *Presidential Leadership. Rating the Best and the Worst in the White House*. New York: A Wall Street Journal Book.

Tuchman, B. (1963/1962). *The Guns of August.* New York: Dell.

Outside-In and Inside-Out Approaches to Transformation

By Richard L. Hughes and Andrew G. Stricker

Abstract

To be successful in the future, organizations will need greater agility, better complex collaboration across organizational boundaries, enhanced collective learning, and overall greater strategic synergy. Efforts to develop such capabilities rarely have achieved desired levels of success, in part because they invariably require real transformation, not just incremental improvement, and because insufficient attention—if any at all—has been given to the leadership and cultural dimensions of transformation. Ongoing research at the Center for Creative Leadership has identified a particular kind of leadership culture that is most naturally adapted to these capabilities—an interdependent or collaborative culture. The center's work also suggests that success in transformation requires significant intentionality in implementing such culture change.

One reason that intentionality is necessary is because new patterns of cultural interaction need to be encouraged persistently. Virtual simulations represent an opportunity to facilitate new cultural behaviors le collaborative learning and interactivity across different parts of functional areas or organizations, some of the very capabilities most organizations are attempting to develop. This essay explores the possible application of virtual reality simulations developed by the U.S. Air Force for individual and organizational learning as part of a transformation effort. Our particular interest here focuses on the optimal features of a simulation designed for practicing shared sense-making, collective learning, and complex collaboration.

189

Introduction

The kinds of capabilities that organizations need to be successful in the face of changing competitive threats and opportunities of the 21st century include greater agility, better complex collaboration across organizational boundaries, enhanced collective learning, and overall greater strategic synergy. Developing these capabilities usually requires fundamental organizational transformation, not merely incremental improvement in current practices.

In contrast, the record of successful organizational transformations over the past several decades is dismal (e.g., Beer & Nohria, 2000a, 2000b; Hirschorn, 2000; Roberto & Levesque, 2005). An examination of many of these attempted transformations indicates that most involved either exclusive or primary emphasis on changes in organizational structure, systems, or processes. Typically there is insufficient attention (if any at all) to the leadership and cultural dimensions of transformation. In the corporate sector, for example, such inattention is considered to be the most common reason for the relatively small proportion of mergers and acquisitions that are actually performed at levels commensurate with original expectations and projections.

It is not the case that changes in organizational structure, systems, or processes are unimportant, it is that they are rarely sufficient. If true organizational transformation is needed, then complementary approaches are called for involving what might be described as both "outside-in" and "inside-out" efforts. Outside-in efforts are changes in structure, systems, and processes that essentially involve conforming behavior to new external (to the person) demands. Inside-out efforts, in contrast, involve changing values, assumptions, and beliefs about how best to achieve effective direction, alignment, and commitment throughout the organization.

One of the reasons that the importance of both outside-in and inside-out approaches to transformation is underappreciated is that although senior leaders and executives invariably recognize the importance of a sound business strategy, few appreciate the critical role that a sound and coherent leadership strategy also must play in successful transformation. Leadership strategy should include at least two main components: an approach to developing the kinds of leaders needed in the "new" organization (e.g., what new competencies should leaders possess?), and an approach to developing leadership in the new

organization that involves more than developing the competencies of individual leaders. For example, leadership development should address the kind of organizational context within which those individual leaders and teams will function (e.g., reward systems, information systems, culture, norms, etc.).

This distinction is useful because for decades organizations have tended to focus their leadership development energies and resources on developing individual leader competencies, often via "leadership development programs." Frequently, however, when individuals returned from such programs (whether offered in-house or via external vendors) to their workplace environments, numerous factors tended to subvert them in their efforts to implement newly learned behaviors. It has become progressively clear in recent years that if organizations want to nurture particular behaviors in leaders, they need to ensure that they have the kinds of formal and informal systems and practices that encourage and sustain (i.e., not just train) such behaviors. Leadership development can be thought of as addressing the fabric of leadership in an organization, and it must involve both outside-in and inside-out elements.

The Role of Culture in Organizational Transformation

One of the most challenging aspects of inside-out transformation concerns an organization's leadership culture. In general, culture can be thought of as a set of unwritten rules or assumptions about "the way things are around here." One thing that makes culture so elusive is its essentially implicit nature. For example, Paparone, Anderson, and McDaniel (2008, 435) write that:

> because mental models are often subconscious and ingrained from many years of indoctrination and socialization, changing these 'theories in use' is not easy. Operators and non-operators alike have entrenched notions of what the military should look like, and each has a deep vested interest in the present way of doing things.

Another factor that complicates an analysis of culture is that in virtually every organization, there are several qualitatively different cultures or mindsets about leadership that are simultaneously, if inharmoniously, present. Ongoing research at the Center for Creative Leadership has identified three particular orientations to leadership that characterize an organization's leadership culture.

Conformer. This cultural orientation is broadly characterized by the assumption that only people in positions of authority are responsible for leadership. This assumption often leads to organizations that emphasize top-down control and deference to authority. In addition, decision-making authority tends to be concentrated in a few senior positions, with seniority and position levels as an important source of status, a conservative approach to change, an emphasis on keeping things running smoothly, and the tendency to publicly smooth over mistakes (also described as a dependent culture).

Achiever. This cultural orientation is broadly characterized by the assumption that leadership emerges as needed from a variety of individuals based on knowledge and expertise. This assumption may lead to decentralized decision-making, high demand for individual responsibility, strong reliance on experts and expertise, and competition among experts. Other characteristics of an achiever orientation include individual performance as an important source of success and status, an emphasis on taking calculated risks, open disagreement, and independent actions within functions or workgroups (also described as an independent culture).

Collaborator. This cultural orientation is broadly characterized by the assumption that leadership is a collective activity requiring mutual inquiry and learning. This assumption may lead to the widespread use of dialogue, collaboration, horizontal networks, valuing of differences, and a focus on individual and collective learning. Other characteristics include the ability to work effectively across organizational boundaries, openness and candor, multifaceted standards of success, and synergies being sought across the whole enterprise (also described as an interdependent culture).

To complicate things further, the same words may be used in these various cultures in reference to quite different kinds of behaviors. Take the very word used to describe the third culture above: collaboration. People in conformer and achiever cultures also obviously talk about collaboration, but they typically mean something essentially different from how it is meant within a true collaborator culture. For example, in conformer cultures, the word may be used to describe "mere" cooperation, such as making certain resources, materials, and so on available to other departments. It typically would not be used to describe cross-departmental, or even cross-organizational, efforts to create shared meaning in the face of ambiguous conditions, as such efforts would not likely even arise in conformer cultures.

A distinction between what has been called simple collaboration and complex collaboration may be helpful here. The distinctions are highlighted in table 1 (Mankin et al., 2004; Hughes and Palus, 2005).

Simple Collaboration	Complex Collaboration
Well-defined task	High task uncertainty
Two people	Multiple people
With much in common	Diverse
Common goals	Different goals and agendas
Face to face	Virtual

Table 1: Simple and Complex Collaboration (Source: Mankin et al., 2004)

In simple collaboration, tasks are routine and well-defined. They are predictable and manageable, and the procedures for addressing them are well understood. Complex collaboration, in contrast, is characterized by tasks that are nonroutine and highly uncertain. The simplest form of collaboration is between just two people, growing more complex as more people are involved. Furthermore, it is not just the number of people collaborating that changes the nature of collaboration; greater diversity among parties also increases complexity, whether it is diversity across points of view, personalities, values, loyalties, or other differences. Differences in goals and objectives significantly increase the complexity of collaborative efforts, and collaboration is simpler and easier when the parties can meet face-to-face. When people in conformer cultures talk about collaboration, it is usually in terms of tasks involving simple collaboration; when people in collaborative cultures do so, it is more often in terms of tasks requiring complex collaboration. It is precisely because conformer and achiever cultures are not well suited to dealing with challenges requiring complex collaboration that many organizations are now striving to develop more collaborative cultures.

In fact, complex collaboration itself may be thought of as just one particular manifestation of more fundamental organizational capabilities of collective learning and general adaptability to dynamic conditions. Behaving in strategically effective ways in an ill-defined yet rapidly changing context requires an adaptive learning capacity by

individuals, teams, organizations, and even networks of organizations. No longer is it sensible to think that behaving in ways strategically important to the organization means merely following deliberate strategic plans prescribing detailed supporting tactics and resource commitments. Increasingly, strategy itself (and by implication its development, communication, implementation, and ongoing refinement/revision) needs to be thought of as an ongoing learning process throughout the organization, rather than as a document (Hughes and Beatty, 2005).

This is consistent with calls for transformation within the military's approaches to strategic leadership (Paparone et al., 2008, 434): "In a turbulent environment, the hierarchically focused strategic leadership will suffice less and less because it cannot respond to changing circumstances in a timely manner. The environment demands the simultaneous adaptation of entire organizations rather than change that trickles down from higher authority."

Rather than placing primary emphasis on a document ("strategic plan"), it may be more helpful to emphasize the kinds of conversations that go on in the organization concerning continuously emerging and strategically significant information and ideas. In other words, "being strategic"—at whatever one's level or function in an organization—depends increasingly on the nature and quality of conversations that one has with others in the organization—conversations that need to be supported through information and other systems, as well as through an organizational culture that values and encourages interdependence and collaboration across boundaries. Effective leadership in the future will depend on continuous learning, and relatively less on what senior leaders know than on their ability to create conditions in which ongoing and pertinent information-sharing and learning throughout the organization is prized and practiced (Hughes and Beatty, 2005). To put it differently, having organizations that are adaptive in the face of dynamic conditions will require, in part, more adaptive forms of organizational culture.

This is important in that the three orientations to leadership culture described here represent different points along a continuum of developmental maturity, such that, generally speaking, the greater the salience of the collaborator orientation in the mix, the greater that organization's capacity is likely to be for coping effectively with complex, ill-defined, and dynamic environments (even when collaborating may not yet be the dominant orientation).

A look at the differing values and beliefs associated with these three distinct orientations helps shed light on the intuitive sense many people share that changing organizational culture is at best a challenging and long-term process (often characterized as taking several years, if not a decade). It is also easy to appreciate that this transformation is aptly thought of as an inside-out change because it involves changing assumptions, beliefs, and values. Some additional factors making culture change so difficult include the difficulty of changing behavior in an environment that outwardly has not changed; marginal levels of proficiency in new behaviors, which may discourage attempts to practice them in a public context; political risks associated with "different" leadership behaviors; and so on.

Given this widely recognized difficulty of changing culture, it may be worth reconsidering the question of whether the cost is worth the gain. Perhaps not surprisingly, there are few empirical studies that shed definitive light on the question. It is worth noting, however, the findings of researchers at the Center for Creative Leadership, whose work on the nature of interdependent organizations provided the basis for the three types of organizational cultures described here. Although the nature of their research (exploratory case studies) prevented definitive conclusions about the causes of organizational performance, the researchers noted two findings that stood out across all the exemplar organizations they studied (McCauley et al., 2008, 43):

- *Organizational learning*. A number of the interdependent practices fostered organizational learning. Across the organizations, more people had access to more information, more shared sense-making was created, improvements to systems and processes were generated, new solutions were created, and organizational change was facilitated.
- *Enhanced organizational capabilities*. The researchers also saw examples of how interdependent practices contributed to enhanced organizational capabilities. Examples included an organization that turned around underperforming, newly acquired units; an organization whose new corporate identity at least partly has overcome its former negative brand identity; and an organization's improved ability to address patient safety problems.

Using Virtual Reality to Facilitate Culture Change and Organizational Transformation

Of all of the characteristics of a collaborative culture, perhaps the one most central to making a successful transformation is collective learning—valuing it and becoming proficient in it. In many ways, collective learning represents the essence of becoming a more collaborative culture. This is true both in the obvious sense that everyone in the transforming organization needs to learn (adapt to and buy into) new systems and behavioral norms, and also in the deeper sense that continuous collective learning is a hallmark of and core competency of a collaborative culture. This raises the question, then, of how best to describe and encourage desired new forms and patterns of interaction in the face of the kinds of barriers to successful culture change noted earlier.

It is no small thing to even adequately describe desired new patterns of interaction, as everyday vocabulary often poorly conveys critical subtleties and nuances. For example, the word *collaboration* is familiar to everyone. However, the connotation of the word to people holding a predominantly achiever orientation may be more or less synonymous with (mere) cooperation, whereas it has a much richer and more complex meaning to people who fully embrace a more collaborative culture. In other words, most people might easily endorse the importance of collaboration, but different people might mean quite different things by their endorsement.

One major challenge, then, would seem to be how best to convey to organizational members just what collaboration, collective learning, sense-making, and so on should look and feel like in the new, transformed culture while simultaneously minimizing the degree of personal and organizational risk associated with performing new behaviors in a clumsy or ineffective manner. One approach for doing that is suggested by recent uses of virtual reality in higher education.

For example, one professor described a new approach to higher education as "virtual conversation," which by its nature seems to "turn passive, knowledge-receiving students into active, knowledge-making students" (Robbins-Bell, 2008, 24). This professor's contrast of the stereotypical lecture hall experience of education with what is happening now in virtual environments seems intriguingly similar to the contrasting natures of predominantly conformer versus collaborator cultures. Perhaps there can be an analogous application of virtual

reality to organizational learning, in which complex collaboration, shared sense-making, and collective learning are practiced in challenging—if simulated—environments. It would be even more valuable if such practice involved not just the opportunity to practice new patterns of interaction but also the very technologies people would be using in their "new" organization (e.g., information technology systems for virtual collaboration).

It is no coincidence that the U.S. Air Force has been actively exploring innovative approaches to individual and organizational learning. Getting the mix of live, virtual, and constructive delivery methods right is essential, and the U.S. Air Force is moving forward quickly in the development of new virtual and constructive simulation capabilities by leveraging existing and emerging technology (Stricker and Clemons, 2009). One such development is the use of virtual worlds and immersive environments to facilitate learning.

Designing a Virtual Simulation for Interdependent Leadership

Virtual simulations represent an opportunity to facilitate collaborative learning and interactivity across different parts of functional areas or organizations. Our particular interest here focuses on the optimal features of a simulation designed for practicing shared sense-making, collective learning, and complex collaboration.

One desirable design feature to achieve such objectives pertains to what might be called the simulation's contextual flexibility. It would seem advantageous to have a virtual world area wherein avatars could freely move about and interact amid relatively lifelike terrain, buildings, and tools and equipment. It would also seem advantageous if the context could support adaptations to the simulation based on specific cultural–geographic or technological contexts, as well as adaptations based on participant performance (Stricker & Clemons, 2009).

A second desirable feature pertains to what might be called the simulation's feedback richness. Individual and group feedback systems would be desirable for supporting such logistical and documentation requirements as assignments of team membership, performance tracking, voice and text communication within and across teams, video recording of activity, and various timing and feedback controls for use by simulation referees (Stricker & Clemons, 2009).

The third desirable design feature pertains to our purpose here in facilitating organizational culture change, and particularly in

developing interdependent leadership. The simulation would need to present interactional and decision-making challenges representative of interdependent leadership that individuals and teams in actual organizations might confront. Furthermore, there would need to be scoring criteria or rubrics for assessing the relative level of interdependent (versus independent or dependent) leadership behaviors that occurred. For example, "beginning," "intermediate," and "advanced" benchmarks could be established by which formal observers of the simulation could assess interdependent leadership behaviors like these, as identified by McCauley et al. (2008):

- soliciting diverse or fresh perspectives from others;
- facilitating or seeking shared sense-making, co-constructing direction, alignment, and/or commitment;
- engaging in dialogue to explore differences;
- actively managing polarities of diverse perspectives;
- openness to revision and change of strategy or approach; and
- engaging in self-authorized decision-making.

In fact, this is just what Stricker and his associates have done. Using the theoretical framework of interdependent leadership described here, they constructed a game sufficiently complex, ill-defined, and dynamic to create a valid laboratory for practicing collective sense-making, learning, and complex collaboration in the context of military decision-making. Their goal was to simulate a naturalistic decision-making environment in which interdependent leadership practices could be experienced and assessed, given that an ill-structured problem or challenge is introduced, the best course of action (COA) is uncertain, competing goals are present, and time pressure and constraints are dynamically put into play. Multiple-event feedback loops are also introduced with unfolding game events, coupled with knowledge-rich sources of additional information presented to the participants by game leaders. The premise is that the key to a successful outcome to the challenge lies in the effectiveness of the participating team's interdependent leadership practices in initially constructing a plausible COA, assessing unfolding events over time, and adapting the COA using a vigilant or hypervigilant decision-making strategy as the situation demands.

Because the incorporation of vigilant and hypervigilant approaches to decision-making is so central to Stricker et al.'s simulation, it is worth exploring those concepts in a bit more detail. Table 2 depicts

differences between vigilant and hypervigilant decision-making strategies (Johnston et al., 1997).

Stricker and his associates reasoned that during most of the simulation, it would be beneficial to switch appropriately between a vigilant and hypervigilant decision-making strategy, depending on changing levels of time pressure and other constraints. Their view was based on the work of Klein (1989), who introduced the recognition-primed decision model.

Vigilant Decision-making	Hypervigilant Decision-making
Decision-maker thoroughly scans all available information	Decision-maker scans only information needed to make an assessment
Decision-maker scans information in a systematic and sequential manner	Decision-maker scans information in any sequence
Decision-maker devotes a consistent amount of attention to each data point	Decision-maker rapidly attends to selected data points
Decision-maker reviews all alternatives before making a decision	Decision-maker reviews needed information only when required

Table 2: Vigilant Versus Hypervigilant Decision-making

Klein (1989) argued that severe time pressures may mitigate against the use of analytic decision strategies, and the recognition-primed decision model describes how decision-makers can intuitively recognize a plausible COA without the use of a multiple options or a detailed analytic decision-making process when under time pressure. Research has shown that intuitive decision-making can result in higher performance than analytical processes (Johnston et al., 1997), and the critical skill seems to be the ability to adapt decision-making strategies to the situation at hand. The design of the simulation described here was based on the notion that a team's successful switching between and use of appropriate decision-making strategies will rest largely on the use of interdependent leadership practices.

The Simulation Scenario

Dr. Andrew Stricker and his team at Air University have been developing an elaborate constellation of virtual reality "worlds" in

Second Life on the Internet. The part of greatest relevance to us here involves the simulation of an international terrorist hostage situation, and it might be helpful to briefly describe the rationale and nature of the simulation while keeping in mind that the actual scenario involves logistical, economic, political, and military complexities similar to those that an actual incident would involve, as well as—importantly for our purposes—both tactical and strategic dimensions. Of course, the specific context, in this case a hostage situation, is relatively unimportant. What is central to the issue of facilitating organizational transformation is creating a simulation that is sufficiently complex, ill-defined, and dynamic to create a valid laboratory for practicing shared sense-making, collective learning, and complex collaboration. Here is the scenario in brief:

> A team of humanitarian workers was taken hostage while on a relief mission to a small island belonging to the country of Murma following a devastating typhoon. The team's response to the crisis was delayed for weeks in no small part because Murma has been under military rule since World War II and has been isolated from the broader international community.

> A small team of relief workers went to find additional survivors in the island's foothills, but they were taken hostage by a group of insurgents opposed to the ruling Murma government and taken to a location in the southern foothills of the island in what appeared to be a war-torn German wolfpack submarine base abandoned after World War II (see Attachment 1). It gradually became clear that the insurgents held ideological beliefs similar to Islamic insurgents. In fact, some of them had been trained and fought as a fundamentalist proxy military force for Al Qaeda. During the insurgents' interrogation of the hostages, they learned that a physician who had been taken captive was the daughter of a very popular ruler of Murma during World War II, though she had fled Murma with her mother decades ago. Her importance to the insurgents increased significantly when her identity and national roots became known.

> The capture of the relief workers by the insurgents soon became known to Murma leaders, and they subsequently demanded that all remaining relief workers immediately leave the island in preparation for the arrival of a Murma military force to attack the insurgents. The Murma leaders expressed little concern for the physician, as she had now been identified as a descendent of the popular ruling family they had removed from power after World War II, and thus was considered a potential threat to the existing military rule.

Given the situational factors of the unfolding crisis, intense negotiations were held involving the Murma leaders, representatives of the United States, and other international leaders. The negotiations resulted in an agreement for a U.S.-led multinational force to land in Murma, prepared to attempt the rescue of the hostages before the planned attack by the Murma military on the insurgent stronghold in the foothills.

This scenario includes both tactical and strategic dimensions, and different virtual reality simulations could be designed emphasizing differentiated learning outcomes appropriate to each. The tactical dimension could involve virtual participation as members of the hostage rescue team (HRT) itself, including specific assignments and constraints given it by the international strategic team overseeing and directing the HRT's work. For example, the HRT could be scored on the basis of the amount of time it takes to rescue the hostages, situational awareness "on the ground," minimizing casualties and collateral damage, HRT group dynamics and collective learning, and so on.

Of greater relevance and interest for our purposes, however, is the potential to design a different simulation focusing on the team monitoring the HRT's actions in Murma. Designing a simulation focusing on this latter team would seem to provide greater opportunity for participants to practice truly collaborative or interdependent leadership. That is because the challenges facing this team (relative to the HRT itself) seem inherently more ambiguous, dynamic, and boundary-spanning in nature. For example, it seems reasonable that strategic oversight of the HRT's mission (e.g., to include a final "go" or "no go" on the rescue itself) should not be scored in quite so definitive a way as scoring for the HRT, as described above. Strategic oversight of the HRT mission could be placed in the broader context of other contemporaneous situations being monitored, as well as the effect that HRT actions in Murma might have on other near-term and long-term U.S. interests elsewhere in the world.

Of course, there is nothing inherent in the specifics of a hostage rescue scenario that is necessary for simulating collaborative or interdependent leadership. Numerous other scenarios could also suffice, including civilian versions, such as managing complex sets of first-responders in a widespread urban catastrophe. Furthermore, if separate tactical and strategic virtual reality simulations were constructed in this manner, whatever the context, it would need to be determined whether

the respective learning outcomes would be enhanced by the two simulations running concurrently (truly a "simulation within a simulation") or independently and separately.

So what might be some possible benefits of a virtual reality simulation like this (more specifically, the strategic version) for facilitating organizational transformation? We can think of several.

Perhaps most obviously, such a simulation would create a practice field for interacting virtually as team members challenged with collective sense-making in a complex and critical, yet ill-defined, situation. It seems beyond question that one of the drivers of organizational transformation today is the need for greater effectiveness in virtual complex collaboration. Systematic feedback could be provided both to individual participants as virtual team members and to their virtual teams as teams, concerning multiple dimensions of their individual and collective effectiveness.

For various reasons noted earlier, it is often difficult to convey in "mere words" what new behaviors and patterns of interaction are expected of people in a new culture or transformed organization. Virtual reality simulations are increasingly lifelike in multiple sensory dimensions, and the ability to create increasingly realistic patterns of social interaction in virtual reality make it possible to depict and practice what interdependent interactions in a transformed organization will look like.

Because organizational transformation is a long-duration process that is inevitably somewhat emergent in nature, results from various "runs" of a simulation could provide useful feedback to the ongoing transformation effort itself. For example, certain kinds of organizational information-sharing practices and information technology systems could be developed and enhanced based on such feedback from the simulation. Of course, one might say, "Why not just get better feedback from the actual work processes of the organization itself? Why do you need a simulation when you can just learn from your actual interactions?"

Perhaps, but in our experience, at least, well-designed simulations, when accompanied with effective debriefing, lead to insights that simply do not commonly arise and are even less frequently voiced in the context of work itself. Such simulation debriefings, which encourage public feedback and both individual and collective learning, can be a vital part of modeling and encouraging precisely the

interdependent leadership behaviors usually desired in a transformation effort.

In the individual and collective learning that could result from the simulation, both facets of a comprehensive leadership strategy for transformation could be served: individual leader development and leadership development (e.g., strengthening key aspects of the desired culture).

Of course, such benefits presume that virtual reality simulations can, in fact, mimic the belief systems and subtle patterns of interaction that are characteristic of the distinctive leadership cultures. Therefore, a first order of business would be to validate whether virtual reality capabilities can support the applications described earlier. Three particular questions would need to be answered in an action research project to validate virtual reality capabilities for this purpose:

1. Can avatars in a virtual reality simulation (i.e., computer three-dimensional versions of simulation participants) reliably portray subtle yet distinctive behaviors that are consistent with the conformer/dependent, achiever/independent, and collaborator/interdependent patterns of culture?
2. Can participants in a virtual reality simulation learn to identify these patterns and control relevant aspects of their (avatar) interactions with others?
3. Under what conditions, if any, does participants' learning in a virtual reality simulation transfer to changed behavior in their actual work organization?

Conclusion

One of the most important elements of a viable and sustainable organizational transformation process is to ensure that organizational members have a clear understanding of the culture and leadership dimensions of the change, as well as to ensure that those valued patterns of behavior are encouraged both formally and informally as the transformation is being implemented. The culture change effort should include an in-depth exploration of the kinds of individual and collective behaviors valued in the new culture with supporting actions to ensure it becomes an internalized, "inside-out" process of personal and collective transformation, as well as an "outside-in" process of merely informing organizational members "how it will be."

Toward those ends, organizations should develop leadership strategies describing the rationale for culture and leadership change, as well as offering training and development opportunities for deepening understanding of and practicing new leadership behaviors. The leadership strategy for culture change could include an exploration not only of what new behaviors are valued, but also why, and an opportunity to explore the implications of acting in the old versus new ways in the face of complex, ambiguous, and changing challenges. Depending on how the three questions posed above are answered, an organization's leadership strategy for facilitating the culture and leadership dimensions of transformation might incorporate virtual reality simulations of shared sense-making, collective learning, and complex collaboration.

This all suggests at least two implications for training and education in the military with regard to developing these capabilities. One of them is somewhat tactical in nature, and the other more strategic. The more tactical implication is that, assuming answers to the three questions warrant it, it would seem useful to develop a variety of training and education virtual reality scenarios representing distinct and targeted points along the range of challenging situations in which, for example, complex collaboration may be required. In doing so, it is likely to be the case that the categorization of collaboration into just the two types suggested in table 1 (simple and complex) is likely to be insufficient for robust training and education efforts. It is easy to imagine intermediate categories of task challenge requiring correspondingly intermediate degrees of individual and organizational collaborative capacity.

A number of such virtual collaboration tasks in network-centric warfare were suggested by Alberts, Garstka, and Stein (1999). Consider one: providing virtual support services from centralized locations by moving information. It seems reasonable to describe that as an example of virtual collaboration on a relatively structured task. We can also imagine, however, scenarios requiring virtual collaboration on highly ambiguous, ill-defined, and dynamic tasks (e.g., the above hostage scenario). It seems likely that training and education efforts to develop individual and collective capabilities in the face of such challenges should need to progress systematically from simpler challenges to more intermediate ones, and only then to the most complex and demanding forms. If we are to use virtual reality effectively in the service of the goals cited at the beginning of this essay—enhancing agility,

encouraging better complex collaboration across organizational boundaries, enhancing collective learning and overall greater strategic synergy—then it may prove useful to design training and education experiences that systematically help students take steps through progressively more challenging kinds of organizational challenges. In other words, not merely design the most sophisticated, challenging, and complex virtual reality simulation possible and "throw them into it" but, rather, develop something like a suite of simulations composed of progressively more challenging conditions.

On the more strategic front (and independent of virtual reality as a training methodology), we should recognize that developing capabilities like enhanced agility, collective learning, and such are not how most Department of Defense educational institutions have historically defined their measures of student success. As with most of higher education, they have tended to define student requirements and success in terms of completing a particular course of instruction (i.e., particular sets of courses with passing grades), rather than in terms of demonstrating particular kinds of individual or collective competencies or outcomes. Yet most of those same institutions are themselves in the midst of something like a sea change in the standards by which they will be held accountable for accomplishing their missions.

Standards of accreditation across virtually all of higher education now include requirements to demonstrate enhancements in student outcomes that transcend particular courses or disciplinary boundaries (e.g., outcomes like critical thinking, oral and written communication, decision-making, teamwork, information literacy, etc.). So we end here with a transformation question for our schools: What would it mean to our Department of Defense educational institutions if they were required to design educational experiences less around which courses students need to take and more to demonstrate enhancements in individual and collective student outcomes? It would seem to mean that our educational institutions themselves are in need of transformation. If our educational institutions are to prepare their students to deal effectively with the challenges of transformation, then those same institutions probably need to change themselves both outside-in and inside-out.

References

Alberts, D.S. et al. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series.

Beer, M. & Nohria, N. (2000a). "Cracking the Code of Change." *Harvard Business Review*, May–June, 133–141.

Beer, M. & Nohria, N. (2000b). "Resolving the Tension Between Theories E and O of Change," in Beer and Nohria, eds. *Breaking the Code of Change*. Boston, MA: Harvard Business School Press, 1–34.

Hirschhorn, L. (2000). "Changing Structure Is Not Enough," in Beer and Nohria, eds. *Breaking the Code of Change*. Boston, MA: Harvard Business School Press, 161–176.

Hughes, R.L. & Beatty, K.C. (2005). *Becoming A Strategic Leader: Your Role in Your Organization's Enduring Success*. San Francisco: Jossey-Bass.

Hughes, R.L. & Palus, C. (2005). "The Development of Effective Collaboration in Organizations." A Connected Leadership Project white paper. Greensboro, NC: Center for Creative Leadership.

Johnston, J.H. et al. (1997). "Vigilant and Hypervigilant Decision Making." *Journal of Applied Psychology*, 82(4), 614–622.

Klein, G.A. (1989). "Strategies of Decision Making." *Military Review*, 56–64.

Mankin, D. et al. (2004). "Developing Complex Collaborations: Basic Principles to Guide Design and Implementation," in *Complex Collaborations: Building the Capabilities for Working Across Boundaries*, Beyerlein, M.M. et al., eds. Elsevier, 1–26.

McCauley, C.D. et al. (2008). "Interdependent Leadership in Organizations: Evidence From Six Case Studies." A Center for Creative Leadership Report, CCL No. 190.

McGuire, J.B. et al. (2008). "Inside Out: Transforming Your Leadership

Culture." *Leadership In Action*, 27(6), 3–7.

Paparone, C.R. et al. (2008). "Where Military Professionalism Meets Complexity Science." *Armed Forces & Society*, 34(3), 433–449.

Robbins-Bell, S. (2008). "Higher Education as Virtual Conversation," *EDUCAUSE Review*, September/October, 24–34.

Roberto, M.A. & Levesque, L.C. (2005). "The Art of Making Change Initiatives Stick." *MIT Sloan Management Review*, 46(4), 53–61.

Stricker, A.G. & Clemons, L. (2009). "Simulation Gaming for Education in MyBase: The Future of Air Force Education and Training With Virtual World Learning." Military Modeling and Simulation Symposium, San Diego, CA.

What do Senior Leaders Need to Know About Cyberspace?

By Jeffrey Caton

Abstract

Cyberspace can be an enabler for beneficial transformation, but it also can be exploited as a dark force to thwart such efforts. International entities cannot extract themselves from cyberspace. What must senior security leaders know about cyberspace to transform their organizations and make wise decisions? How does the enduring cyberspace process interact with and transform organizations, technology, and people, and, in turn, how do they transform cyberspace itself?

To evaluate these questions, this essay establishes the enduring nature of the cyberspace process and compares this relative constant to transformation of organizations and people. Each section discussing these areas provides an assessment of their status as well as identifies key issues for senior security leaders to comprehend now and work to resolve in the future. Specific issues include viewing cyberspace as a new strategic common akin to the sea, comparing effectiveness of existing hierarchies in achieving cybersecurity against networked adversaries, and balancing efficiency and effectiveness of security against the universal laws of privacy and human rights. Finally, leaders need to scan the strategic horizon for potential cyberspace-related technological and societal trends and shocks and provide clear visions for success to their organizations.

Introduction

The growth of worldwide cyberspace-related capabilities is a double-edged sword. Cyberspace can be used as an enabler for beneficial transformation, but it also can be exploited as a dark

207

force to thwart such efforts. [1] Senior security leaders must deal with both sides, and with increasing frequency and greater risks to their missions. Simply put, international entities cannot extract themselves from cyberspace. Given this, what must senior security leaders know about cyberspace to transform their organizations and make wise decisions? How does the enduring cyberspace process interact with and transform organizations, technology, and people, and in turn, how do they transform cyberspace itself?

This essay addresses broad applications of the cyberspace process across diplomatic, informational, military, and economic communities worldwide. Although it discusses technological implications, it avoids detailed technical aspects that might detract from the strategic nature of the content.

To evaluate the central questions posed here, this essay establishes the enduring nature of the cyberspace process and compares this relative constant to transformation of organizations and people. Of course, none of these dimensions exist in isolation—the analytical simplification of evaluating one variable at a time enhances focus and readability. Each section provides an assessment of the status of the dimensions and identifies key issues for senior security leaders to comprehend now and work to resolve in the future.

Background

The term *cyberspace*[2] often carries an aura of mystery that may belie its fundamental nature. Many respected authors assert that cyberspace and its applications are revolutionary. Rather than argue this point, I posit that the basic process governing cyberspace is defined

---

[1] The following definitions are used for this chapter: *Cyberspace* is (1) a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (England 2008) and their operators; (2) a new strategic common, analogous to the sea as an international domain of trade and communication (Cebrowski 2004). *Transformation* is a process that shapes the changing nature of competition and cooperation through new combinations of concepts, capabilities, people, and organizations (Rumsfeld 2003, 3)

[2] Science fiction author William F. Gibson is credited with coining the term "cyberspace" and popularizing it in his book *Neuromancer* (Gibson 1984)

easily. Further, when viewed as a "strategic common," cyberspace indeed shares many characteristics with the sea, but it also has unique ones as well (Cebrowski, 2004). These distinctive aspects relevant to security within cyberspace are the focus of this essay.

In its simplest form, the cyberspace process consists of three elements—cognitive, informational, and physical (Woolley, 2006). For example, someone generates and articulates a thought (cognitive), and enters the thought into a communication device (physical), where it becomes a systematic representation of data (information), possibly represented digitally using electromagnetic means. Next, the data travels through a variety of physical lines of communication (e.g., telephone, cable, fiber optic line, radio, microwave, etc.), where it exits through a communication device to another user for cognitive use, or perhaps to a physical device to perform an operation (e.g., turn on a light, open a valve).

What is cyberspace, then? It is the sum total of all elements required for cyberspace processes to occur. The fundamental structure of the cyberspace process is enduring, but the configuration of cyberspace itself transforms when specific elements of the basic process transform. This is an essential concept for the analysis of cyberspace transformation addressed in this essay.

To illustrate this further, let us consider the evolution of the cyberspace process since the invention of electromagnetic transmission. As depicted in figure 1, the telegraph is an early example of the cyberspace process. An operator would read a message and enter it as data (Morse code) using a simple switch that sent pulses of electric current to a remote receiving switch, where a different operator would decode the taps into the original message. This basic process evolved in scope and complexity for over 100 years. In the mid-twentieth century, the process was transformed with the introduction of electronic transistor-based data-processing devices.
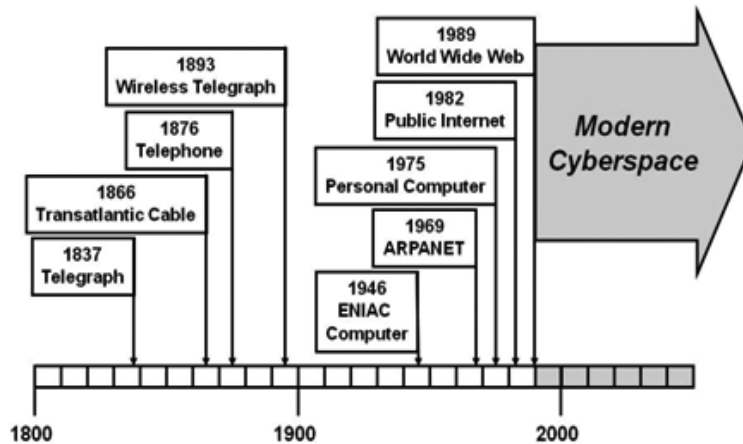
Figure 1: A Brief Timeline of Cyberspace Development

I posit that although the cyberspace process has existed for centuries, cyberspace as currently envisioned came into existence with the introduction of the personal computer (circa 1975), the Internet (circa 1982), and the World Wide Web protocol (circa 1989). The synergy of these events established cyberspace as a new strategic common analogous to Mahan's theories in which the sea is described as "a wide common" that was the international domain of commerce and communication (Cebrowski, 2004). Similarly, cyberspace can be mapped using techniques that clearly show its lines of communication and critical nodes with tactical, operational, and strategic implications for their control.[3] The Cooperative Association for Internet Data Analysis in San Diego, California, is pioneering the macroscopic measurement and analysis of Internet performance, developing several practical maps of topology, security, routing, and other aspects (Claffy et al., 2008). When combined with innovative graphical depictions, these maps clearly show nodes and choke points—the cyberspace equivalent of the Straits of Hormuz or Malacca (Cooperative Association for Internet Data Analysis, 2009). The security of these critical nodes—some of which may be physical, others informational—

---

[3] Dodge and Kitchin (2001) conducted a 5-year study of cyberspace maps and spatializations created by academic and commercial organizations and compiled their results in *Atlas of Cyberspace*.

should be of great interest to anyone attempting to protect or exploit cyberspace.

Given such similarities among the two strategic commons, cyberspace has at least five unique characteristics of concern to senior security leaders. First, the cost of entry and routine access to cyberspace is extremely low—basically the cost of a laptop and Internet café fee. Second, cyberspace offers a degree of anonymity that greatly challenges efforts to detect, track, and target a user who desires to hide in the common.[4] Third, cyberspace provides the ability to initiate a wide variety of physical effects across vast distances at almost instantaneous speeds. Fourth, cyberspace is an ever-growing common—every new computer server or Internet-capable cell phone expands its boundaries. Finally, cyberspace does not have traditional dimensions of height, depth, and length, but it does have unique metrics that can be used to map its boundaries and operations.[5]

What types of threats exist in this new common? In general, attacks in cyberspace fall into one of three categories—the interception, modification, or denial of information (Woolley, 2006). Attacks may be overt or covert, with kinetic or nonkinetic effects. The damage inflicted varies greatly, from defaced Web sites to multi-million-dollar financial losses, and even to actual physical damage to equipment, the control of which is connected to cyberspace. How do leaders transform their organizations to address these challenges?

Organizations and the Cyberspace Process

The United States clearly recognizes that cyberspace security (also called cybersecurity) is essential to its overall national security and that it has implications across all instruments of national power—diplomatic, informational, military, and economic. The U.S. strategic

---

[4] Some may argue that individuals may hide in physical space among a population of billions with equal anonymity, such as that offered by cyberspace. Although a full debate exceeds this chapter's scope, some of the unique features facilitating anonymity in cyberspace include the ability to enter and exit the common, the ability to create and control multiple versions of the user's presence, and the ability to take over another user's identity (usually without their consent or knowledge)—all accomplished with no change to the user's actual physical attributes.

[5] Note that this is one area where the author disagrees with Cebrowski's view that the cyberspace common is dimensionless (Cebrowski 2004).

objectives for accomplishing this security are to prevent cyberattacks, reduce national vulnerability to cyberattacks, and minimize damage and recovery time, should attacks occur. Equally important, the need to have a secure cyberspace involves the international community. The United States explicitly states this in two of its five national priorities for its cyberspace strategy—securing governments' cyberspace and international cooperation (Bush, 2003).

This section addresses how organizations interact and innovate to transform their own structures to meet the security challenges of cyberspace. The discussion steps though each of the four major instruments of national power to assess their status and identify issues for senior security leaders to comprehend and work to resolve.

Diplomatic

How should countries interact in cyberspace? Does this new common require entirely new standards of conduct? As independent governments, they have an international obligation to act in good faith and settle disputes with other states by peaceful means. If conflict should occur, the right of using proportional force in self-defense is a cornerstone of international security. Sharp (1999) argues that "it now seems almost universally accepted that a considerable body of international law does indeed apply to the use of force by states in CyberSpace."

However, the widely distributed nature of cyberspace does not necessarily recognize national boundaries, and new provisions to address this reality seem prudent. Arguably, the most significant event moving us toward defining acceptable cyberspace interactions is the Council of Europe Convention on Cybercrime, a formal agreement among 43 countries "to better combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation" (Archick, 2006, 1). The convention began in 1997, was opened for signature on November 23, 2001, and has been ratified by at least 16 countries. Its provisions include definition of criminal offenses in four categories (fraud and forgery, child pornography, copyright infringement, and security breaches), as well as methods to address these crimes, such as investigation and extradition procedures (Archick, 2006).

The U.S. Department of Justice has arrested and convicted domestic and international individuals and small groups committing cyberspace-

related crimes since 1998.[6] The department determines whether the crime targeted a private individual or corporation or a government agency, as well as whether the crime posed a threat to public health or safety (e.g., power grids, air traffic control) (U.S. Department of Justice, 2009). The attackers included citizens from China, Russia, Kazakhstan, Israel, and the United Kingdom. In some cases, extradition requests were pursued per the Convention on Cybercrime (Anonymous, 2009).

Informational

How can information be stored safely in cyberspace? The U.S. Government views information technology as one sector of the nation's critical infrastructure and has tasked the Department of Homeland Security with its protection. In turn, the Department of Homeland Security created a National Cyber Security Division in June 2003 to serve as a focal point for cybersecurity issues. Working to avoid information-sharing failures such as those that contributed to the September 2001 terrorist attacks, the Department of Homeland Security conducted 16 major cyber exercises between 2004 and 2008. To practice and enhance collective responses to cybersecurity scenarios, the exercises included participants from federal, state, and local governments, as well as participants from private industry, academic institutions, and foreign governments (U.S. Government Accountability Office, 2008).[7]

In January 2008, President Bush signed Homeland Security Presidential Directive 23, better known as the Comprehensive National Cybersecurity Initiative. The initiative is a classified document, but three of its major "public" priorities directly support the access points, data traffic, and security protocol for information traversing U.S.

---

[6] The fact that the U.S. Department of Justice claims jurisdiction for cyberspace crimes having physical effects on U.S. individuals and organizations is not the same as suggesting there is a "U.S. cyberspace boundary." The details of physical and virtual national sovereignty deserve further debate.

[7] Cyber Storm II description: Sponsored by the Department of Homeland Security, this exercise was to improve national incident response and coordination capabilities by simulating physical and cyber attacks against the transportation, information technology, and chemical critical infrastructure sectors. Participants included federal, state, and foreign governments and private industry (General Accounting Office, 2008).

Government agencies' computer networks. First, the Trusted Internet Connection effort is simply a way to prevent cyberattacks by reducing the number of access points. Next, the Einstein II program automatically monitors the data traffic within the networks and Internet access points. Third, the Federal Desktop Core Configuration program mandates a common security protocol for government desktop computer systems (Lake, 2009).

Military

How are traditional military organizations embracing operations within the cyberspace domain? In his recent testimony before the U.S. Congress, Secretary of Defense Robert Gates (2009a, 8) acknowledged the extent of the threat:

> With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DOD's vast information grid—a system that encompasses more than 15,000 local, regional, and wide-area networks, and approximately 7 million [information technology] devices.

To address this issue, Secretary Gates designated cyberspace as one of the four focus areas in the recent Quadrennial Roles and Missions Review (Gates, 2009b), a reinforcement of tenets in his 2008 National Defense Strategy (Gates, 2008). The goal is to establish the foundation for developing capable cyberspace forces; structure the forces, as well as their processes and procedures; and then employ these forces to achieve desired effects across the full range of military operations. The study's Cyber Issue Team emphasized the need "to learn from new, innovation capabilities and experiences of our counterparts across the U.S. Government, in the private sector, and internationally" (Gates 2009b, 16).[8]

In April 2007, the Estonian government, commercial, and private organizations endured 3 weeks of cyberattacks. Responding to a historic request by a member state of the North Atlantic Treaty Organization (NATO) in defense of its digital assets, the United States sent computer security experts to Estonia to help with recovery efforts

---

[8] The stated Department of Defense vision is to develop cyberspace capability that provides global situational awareness of cyberspace, U.S. freedom of action in cyberspace, the ability to provide warfighting effects within and through cyberspace, and when called on, provide cyberspace support to civil authorities (Gates 2009b, 14).

(Geers, 2008). The aftermath of this attack included the creation of two new cybersecurity organizations. First, at the operational level, the Cyber Defence Management Authority was established in Brussels, Belgium, to provide a centralized bureau for coordinating Alliance response to any further cyber attacks (Hughes, 2009). Second, at the strategic level, the Cooperative Cyber Defence Centre of Excellence was established at Tallinn, Estonia, with a mission "to enhance the cooperative cyber defence capability of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence" (Cooperative Cyber Defence Centre of Excellence, 2009).

Economic

What are the costs to industry of cybersecurity breaches? How can these costs be quantified and evaluated so business firms can adopt the measures that provide the most cost-effective solution? The stakes are high—a recent report surveying senior information technology decision-makers from over 1,000 large businesses and security firms estimated that companies lost an average of US$4.6 million worth of intellectual property in 2008 (McAfee, 2009). The latest Annual Threat Assessment of the Intelligence Community estimates total cyber-related business losses in 2008 to be US$42 billion for the United States and US$140 billion globally, as well as possibly US$1 trillion worth of intellectual property lost globally (Blair, 2009). Even determining when an attack occurs in business is difficult, and it is even more challenging to measure the cost of attacks. However, investigations into effects on stock price following cyberattacks indicate that targeted firms suffer short-term losses of 1% to 5%, which could translate into shareholder losses of as much as US$200 million (Cashell et al., 2004).

Three major market forces compel businesses to manage their cybersecurity—competition, liability, and insurance. Firms that establish best practices for cybersecurity will be rewarded in a competitive market. Reduced cyberattacks lead to increased consumer confidence, as well as a healthy net profit. If these benefits are not sufficient, then liability, specifically the prospect of potential legal actions for compromised confidential consumer information, is a strong motivation. Finally, profit opportunities are emerging for cyber-risk insurance. Both the company buying such insurance and those supplying the service stand to profit, as they have in similar economic ventures (Cashell et al., 2004).

Cyberspace Issues for Organizational Transformation

How should senior security leaders address the challenges posed to current organizations by the dynamic activities in cyberspace? Will traditional approaches and structures suffice, or are new organizations required? Rather than delve down to the tactical level, let us address these questions at the strategic level, focusing on three tenets—credibility, balance, and hierarchy of organizational transformation to incorporate cyberspace.

From the preceding discussion, it is clear that security in cyberspace is an issue affecting all instruments of national power. The recent report, *Securing Cyberspace for the 44th Presidency* (Langevin et al., 2008, 15), lists as one of its three major findings that, "The United States must treat cybersecurity as one of the most important national security challenges it faces. … This is a strategic issue on par with weapons of mass destruction and global jihad."

If organizations are to achieve credibility in such security efforts, then they need to articulate the expressed risks in consistent and objective terms. For example, when cyberspace is viewed as the new strategic common, comparing security in cyberspace to issues like weapons of mass destruction is no more applicable than a comparison with security of the sea. Perhaps a way to articulate security issues for cyberspace more effectively is to couple the strategic common construct with the current U.S. model of challenges—traditional, irregular, disruptive, and catastrophic (Rumsfeld, 2006). Although there are, no doubt, potential "nightmare scenarios" that can be constructed within cyberspace, their roles need to be assessed objectively by considering the possible outcome in concert with its feasibility and probability of occurrence. Then the concern expressed in the previous quotation can be reworded to achieve credibility of purpose; "Although unlikely, the catastrophic cyber attack on our military networks is a strategic issue on par with weapons of mass destruction."

Unlike the other strategic commons, cyberspace has direct and regular interface with a vast numbers of people in over two hundred countries (Central Intelligence Agency, 2008). At a United Nations Internet Governance Forum in November 2007, a key participant noted, "the dilemma between Internet freedom and Internet regulation could be resolved by striking a balance among the various competing interests" (U.N. News 14 November 2007). In this context, the opposing sides of the scale are security versus personal privacy.

Despite the international security benefits achieved by the Cybercrime Convention, some organizations petitioned U.S. senators to oppose its ratification, asserting it "lacks adequate safeguards for privacy" and has "insufficient recognition of international human rights obligations" (Rotenberg & Laurant, 2005). Although this opposition did not prevent ratification, its espoused principles deserve continued attention by strategic leaders as they transform organizations. Consistent with this, the October 2007 U.S. National Strategy on Information Sharing specifically establishes "Protecting Privacy and other Legal Rights" as its foundation, which includes foreign partners in this tenet. In addition, it explicitly links these principles to the pursuit of other national strategies, including homeland security and combating terrorists (Bush, 2007).

How should senior security leaders organize their resources to address the full spectrum of cybersecurity challenges? In an ironic twist, a recent report (Langevin et al., 2008) recommended in general terms that the U.S. Government move toward an information-age government that uses cyberspace and social networking, yet the report also recommended at least five new industrial-age organizations in the short term. Conti and Surdu (2009) argue for a new cyberwarfare branch of the U.S. military but fail to articulate what mission it would fulfill. It is doubtful that such traditional bureaucratic structures can keep pace with the rapidly evolving nature of cyberspace. Arquilla and Ronfeldt (2001, 15) are direct in their assessment: "hierarchies have a difficult time fighting networks," and groups organized in networks pose many of the challenges in cyberspace. Although more responsive and better suited for countering dynamic threats, transforming current security organization into network-based structures requires leaders who are comfortable with flexibility and dispersed authority.

People and the Cyberspace Process

Having looked at the various organizations and instruments of power at work within cyberspace, let us consider the individuals who operate there. This section first focuses on people who choose to conduct illegal activity in cyberspace. Next, it examines the connectivity and attitudes of people using cyberspace and concludes with a look at various factors affecting the mutual transformation of people and the cyberspace strategic common.

Wrongdoers in Cyberspace

Who are the perpetrators of illegal activity in cyberspace? To analyze the diversity of cyberspace lawbreakers, let us consider four categories of these individuals (who may also work in groups)—cyber-delinquents, cybercriminals, cyberspies, and cyberterrorists. Each set of perpetrators differs in attitudes and actions regarding ideology (e.g., political or religious), monetary gain, attribution, knowledge-sharing, and destruction of societal structures. One common interest among all but the most extreme individuals (e.g., anarchists) is the preservation of cyberspace infrastructure—they all have a vested interest in maintaining the domain from which they derive power.

Think of cyber-delinquents as the thrill seekers of cyberspace. Their primary motivation is to cause trouble that is highly visible in cyberspace, and perhaps in the world in general as well. To demonstrate their brilliance and "share the fun," they are more likely to provide their trade secrets for beating cyberspace security. Ideology and monetary gain may play a role in their psyche, but they do not dominate. Although not their intent, some of their pranks may inadvertently endanger public safety (e.g., changing traffic signals) or violate very severe laws, such as possible child pornography in the recent cases of "sexting" among teens (Hamill, 2009). In the grand scheme of cyberspace security, cyber-delinquents are regrettable nuisances.

In contrast, consider cyber-criminals, operators focused primarily on monetary gain. They have little regard for ideology and destruction of societal infrastructure unless they are acting in a mercenary role. Obviously, they do not want to be known, as that increases their probability of arrest, and they are not apt to share the techniques they use to turn a profit. In strategic terms, they are a growing threat to economic power. The 2008 CSI Computer Crime and Security Survey noted the disturbing trends of cybercriminals becoming more professional in their crimes, clearly separating themselves from cyber-delinquents' pursuit of "bragging rights." Cybercriminals have become stealthier by exploiting the inherently reactive nature of defensive security measures, as well as more sophisticated in the targeting of their attacks. The most expensive attacks were those of financial fraud, with an average reported cost of over US$463,000 per incident (Richardson, 2008). In broader terms, criminals stole data from over 47 million credit and debit cardholders by hacking retail marketers (Housman, 2009).

Next are the cyberspies—operators driven by ideology, usually of a specific government. Similar to the cybercriminals, they seek to remain anonymous in their deeds and capabilities, but they may share information with other cyberspies for mutual benefit. They may cause no overt damage in their activities, opting to monitor information rather than intercept it. By constantly probing and scanning critical nodes of other countries' cyberspace infrastructure, they can identify vulnerabilities to be extorted or exploited during a time of crisis or conflict. The scope of such activity is staggering. Wilson (2008) cites U.S. Department of Defense officials' estimates of the military global information grid experiencing more than three million daily scans, as well as counterintelligence officials' estimate that 140 different foreign intelligence agencies regularly attempt to hack into U.S. commercial and government computers.[9]

Finally, there are the cyberterrorists, who are motivated by political or social ideology but also by the desire to be recognized for their deeds to aid in recruiting followers or gaining perceived legitimacy (including possible state sponsorship). They work effectively in a network structure and are likely to share much of their knowledge regarding how to conduct terrorist operations in the hope of spreading their influence. Monetary gain through cyberspace crimes may not be a direct motivation for cyberterrorists, but it may help fund their activist agendas. Because they can exercise significant power and influence though cyberspace, one could argue that it is unlikely that they will cause widespread damage to its supporting infrastructure.

Connectivity

Innovations in computer technology have greatly enhanced the ability of the average citizen to operate freely in cyberspace. Data processing speeds and digital storage media continue to grow exponentially (Ekman et al., 2004), with competitive markets that drive sales prices down. The United States accounts for over 22% (over 264 million) of all personal computers in the world (over 1.19 billion; Computer Industry Almanac, 2009), but China recently surpassed the United States in the number of Internet users (253 million versus 220

---

[9] In April 2009, the *Wall Street Journal* reported alleged activities in which cyberspies from China, Russia, and other countries "were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war" (Gorman 2009).

million; Anonymous, 2009). With 222 countries having Internet access, 86 of which have at least one million users (Central Intelligence Agency, 2008), it is becoming difficult to find any place in the world not affected by cyberspace. In fact, the United Nations recently sponsored an Internet governance conference with attendees from over 100 governments, with two of the five main topics focused on "reaching the next billion with Internet access" and "the Internet of tomorrow" (U.N. News, 2008b)

Because the cyberspace process includes physical elements, it is not surprising that industry and government leverage the ability of cyberspace-based remote access to control infrastructure. Usually called Supervisory Control and Data Acquisition (SCADA) systems, these control processes increase operational effectiveness and efficiency for many applications to include such systems as electric power, oil, gas, transportation, and telecommunications (Varnado, 2005). Often, older SCADA devices were designed and installed without regard for security, and most new SCADA systems use the Internet to pass control information. As the worldwide population of Internet users pushes toward two billion, it is wise to pursue better security promptly for any physical systems accessible via that portion of cyberspace.[10]

Attitudes

Is the increasing individual and collective access to cyberspace creating its own unique cyber-ethos? How is this transforming the interactions among people and groups? Certainly, the current generation of Internet users is diverse, but many are using cyberspace to bridge gaps in language and culture. Social networking Web sites, such as Facebook and MySpace, attract around 115 million unique visitors each month, demonstrating a willingness to place personal information online (Arrington, 2008). There are also many new avenues of immediate communication available to users—such as instant messaging, blogs, and Twitter—that are accessible through a myriad of hard-wired as well as wireless devices (e.g., cell phones, personal digital assistants, laptops, etc.).

---

[10] The U.S. Department of Energy reported on recommended changes to power-generation facilities resulting from a U.S. Department of Homeland Security experiment in March 2007. The test demonstrated the ability to cause catastrophic physical damage to an industrial turbine via commands sent through its SCADA system (DOE 2007).

The ubiquitous nature of the virtual social world facilitated by these devices often causes problems in "real" society. In the interest of public safety, many U.S. states outlawed the use of cell phones for motor vehicle drivers, and sometimes the law specifically restricts text messaging (Governors Highway Safety Association, 2008). The potentially devastating effects of "cyber bullies" are also being scrutinized, especially in light of tragic events where it may have contributed to an individual's death, such as a recent teenage suicide in Missouri (CBS News, 2008). It is reasonable to expect new social and ethical issues for the cyberspace common as it continues to expand into global society.

Cyberspace Issues for Transforming People

Does the transforming nature of cyberspace present new challenges for senior security leaders in their interactions with people, or will status quo interpersonal dynamics suffice? To evaluate this, let us focus on three strategic topics—trends, leverage, and synthesis of technologies and individuals—and the implications of transforming their interactions in cyberspace.

At risk of stating the obvious, it is important for senior security leaders to realize and embrace the future trends of cyberspace. With regard to people, they must fully understand the ramifications of the current generation of students entering university. Given the start of modern cyberspace posited in this essay, these students know no other world than that of billions of computers and Internet users. What is a revolution for senior leaders is status quo to them.

Consider the recent U.S. presidential election. BBC News (Schifferes, 2008) reported on Barack Obama's campaign success in using the Internet for fundraising and communication as representing a sharp departure from traditional phone call tactics. Although viewed as innovative among older voters, newly registered voters may respond simply, "Of course these techniques were used—how else do you communicate?" This example illustrates how different generations view and apply readily available cyberspace tools. As senior leaders seek to recruit and develop people in their organizations, they should not limit their focus to fulfilling the needs of today's cyberspace activities but, rather, should look at least several decades into the future to envision and pursue the talents and skills required for a transformed cyberspace common. However, they need to remember that not everyone operating in cyberspace has lawful motives.

What types of skills and technology can people leverage to their advantage within cyberspace? Individuals in the four broad categories of cyberspace wrongdoers may interact for mutual benefit, or they may exploit law-abiding operators. Wilson (2008) identifies cases in which cyberterrorists employed cybercriminals to steal credit card information and support drug traffickers, all toward the goal of funding traditional terrorist operations. Another lucrative business is the marketing of "botnets"—virtual armies of compromised computers that can be controlled remotely over the Internet by a "botmaster." Botnets may exploit hundreds of thousands of computers, usually without the owners' knowledge (Wilson, 2008). An adversary with such capability, if coupled with a network structure, could achieve swarming attacks and defenses—in cyberspace as well as other strategic commons—that challenge the "traditional mass- and maneuver-oriented approaches to conflict" (Arquilla & Ronfeldt, 2001, 12).

As the cyberspace capabilities increase, the methods used to develop individual skills to leverage these capabilities transform. User interfaces have progressed significantly over the past two decades, incorporating visual icons and common menu structures that allow even novice users the ability to master new applications in hours, if not minutes, without any formal training. If problems occur, the "help" menus offer advice and tutorials, often supported by extensive online databases. Unfortunately, not all "self-help" is benevolent. Cyber wrongdoers can develop and enhance their illegal skills using online "how to" information that may be updated rapidly to counter new security measures. To meet this challenge, senior leaders may need to transform traditional education, training, and certification programs for their cybersecurity workforce and emphasize continuous training using decentralized network techniques. As Arquilla and Ronfeldt (2001, 15) concluded, "whoever masters the network form first and best will gain major advantages."

How will people and their leaders cope with the cyberspace common's expansion, as well as its supporting technologies that grow at geometric rates? Although existing WiFi and Bluetooth technologies have removed the bonds of cables and lines for many users, ongoing research and development offers further possibilities for removing cumbersome computer display and input devices. This ultimate degree of connectivity with almost no personal physical infrastructure is still ahead, perhaps in the near future.

Consider the synthesis of combining proven and feasible technologies to enhance the human–machine interface. Over 112,000 people worldwide have cochlear implants—a transmitter and receiver device that stimulates the auditory nerve in deaf patients to simulate nature hearing processes (National Institute on Deafness and Other Communication Disorders, 2007). Similar principles were used to develop a self-contained artificial silicon retina microchip, which is implanted in the human eye to help mitigate retinal degeneration (Optobionics, 2008). Starner and Paradiso (2004) present several viable options for human-generated power for operating mobile electronics, most based on normal body motion (e.g., walking, breathing, body heat, etc.). By combining these technologies and adding fingertip sensors for data entry purposes, it is conceivable that their synthesis could result in people who have a fully self-contained direct interface to cyberspace. Certainly, this could raise even more challenging issues of security and privacy, given the potential for every individual with optical implants to become a walking Web camera.[11]

If this ultimate connectivity comes to fruition, it may have pronounced effects on many individuals. A survey by Anderson and Rainie (2006) postulates it may exacerbate two extreme attitudes within the population—addicts and luddites. The addicts are those individuals who devote most of their time to living in synthetic worlds. Often disguising their true nature and characteristics by appearing as self-designed "avatars," the prospect of almost complete sensory immersion into cyberspace may cause them to retract further from real-world society. In contrast, luddites are individuals who oppose technological change. The radical measures of achieving ultimate connectivity may create such a change in society as to compel violence from such individuals who refuse to participate. Some in the survey also worried that technology may eventually create machines and processes that move beyond human control. Although this notion has been the theme of many works of fiction over more than a century, the continued rapid growth of cyberspace systems' capability and complexity now makes it a legitimate concern for organizational leaders.

---

[11] Perhaps the most radical approach in such an environment would be to adopt a doctrine of total transparency—basing plans and operations on a central assumption that all users can see all information at any time. Although thought provoking, the implications of this concept are beyond this chapter's scope.

Conclusion

Clearly, the dawn of modern cyberspace introduced a myriad of challenges, only a small sample of which were discussed in this essay. I offer five closing thoughts on the central theme of what senior security leaders must know about cyberspace to transform their organizations and make wise decisions. First, they should avoid the mystery surrounding cyberspace and embrace it as a new strategic common of communication and commerce akin to the sea. They should recognize and plan for its security across all instruments of national power—diplomatic, informational, military, and economic. Next, it is doubtful that existing hierarchies will be effective in achieving cybersecurity against networked adversaries. Leaders need to consider adopting similar dispersed network principles to transform their organizations to be more agile and less vulnerable. Third, leaders should not lump all adversaries together but, rather, recognize that they may have common motivations and self-imposed restrictions regarding how they operate in cyberspace. These groups have the capability to interact over vast distances with each other as well as to exploit unwilling users in ways that increase their collective ability to affect cyberspace operations. Next, although there is a trend toward greater sharing of personal information via social networking, the measures that leaders direct to meet cyberspace challenges need to balance the efficiency and effectiveness of security against the universal laws of privacy and human rights. Finally, leaders need to scan the strategic horizon for potential cyberspace-related technological and societal trends and shocks and provide clear visions for success to their organizations.[12]

---

[12] Since the original presentation of this essay, three significant events have occurred in the United States. First, on May 29, 2009, President Obama announced the creation of a new White House office led by a Cybersecurity Coordinator as well as five key areas for action. The coordinator will be a member of both the National Security Staff and the National Economic Council. It is interesting to note that President Obama mentioned that his staff's computers were hacked during the general election campaign (Obama 2009). Second, on June 23, 2009, Secretary of Defense Gates directed the development of a new national strategy for cybersecurity as well as the establishment of U.S. Cyber Command as a subordinated unified command under U.S. Strategic Command. He specified an initial operating capability not later than October 2009 and full operating capability by October 2010 (Gates 2009c). Third, on July 4, 2009, there was a wave of cyberattacks aimed at American and South Korean government and commercial Internet sites.

References

Anderson, J.Q. & Rainie, L. (2006). *The Future of the Internet II*. Washington, DC: Pew Internet and American Life Project. Available from http://www.pewinternet.org [Accessed March 31, 2009].

Archick, K.. (2006). *Cybercrime: The Council of Europe Convention*. CRS Report for Congress RS21208. Washington, DC: Congressional Research Service.

Arquilla, J. & Ronfeldt, D. (2001). "The Advent of Netwar (Revisited)," in Arquilla and Ronfeldt, eds. *Networks and Netwars*. Santa Monica, CA: RAND, 1–25.

Arrington, M. (2008). "Facebook No Longer The Second Largest Social Network." *Tech Crunch* June12. Available from http://www.techcrunch.com [Accessed April 1, 2009].

Blair, D.C. (2009). *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence*. Washington, DC: Director of National Intelligence.

Bush, G.W. (2003). *The National Strategy to Secure Cyberspace*. Washington, DC: White House.

Bush, G.W. (2007). *National Strategy for Information Sharing; Successes and Challenges in Improving Terrorism-Related Information Sharing*. Washington, DC: White House.

Cashell, B. et al. (2004). *The Economic Impact of Cyber-Attacks (CRS Report for Congress RL-32331)*. Washington, DC: Congressional Research Service.

CBS News. (2008). "Woman Indicted in Cyber-Bully Suicide." May 15. Available from http://cbsnews.com [Accessed April 1, 2009].

Cebrowski, A.K. (2004). "Transformation and the Changing Character of War? Transformation Trends." Available from http://www.afei.org/transformation [Accessed March 27, 2009].

Central Intelligence Agency. (2008). "Country Comparisons—Internet Users," in *The World Factbook*. Available from https://www.cia.gov/library/publications [Accessed March 31, 2009].

Officials and experts stated that at least 27 sites were targeted by botnets of 50,000 to 65,000 computers. Assessments of the attack ranged from "unusually resilient" to "garden-variety" (Sang-Hun & Markoff 2009).

Computer Industry Almanac. (2009). "PCs In-Use Reached nearly 1.2B in 2008; USA Accounts for Over 22% of PCs In-Use." News Release January14. Available from http://www.c-i-a.com [Accessed March 31, 2009].

Cooperative Association for Internet Data Analysis. (2009). *Data Collection at CAIDA—Research Topics*. San Diego, CA: Cooperative Association for Internet Data Analysis. Available from http://www.caida.org/data/ [Accessed March 31, 2009].

Cooperative Cyber Defence Centre of Excellence. (2009). *Mission and Vision*. Tallinn: Cooperative Cyber Defence Centre of Excellence. Available from http://transnet.act.nato.int/WISE/TNCC/ CentresofE/CCD [Accessed March 30, 2009].

Claffy, K. et al. 2008. *Internet Mapping: From Art to Science*. San Diego, CA: Cooperative Association for Internet Data Analysis.

Conti, G. & Surdu, J. (2009). "Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?" *IAnewsletter*, 12(1), 14–17.

Dodge, M. & Kitchin, R. (2001). *Atlas of Cyberspace*. Harlow: Pearson Education.

Ekman M. et al. (2004). *An In-Depth Look at Computer Performance Growth (Technical Report 2004-9)*. Goteborg: Chalmers University of Technology.

England, G. (2008). "Memorandum: The Definition of 'Cyberspace.' " Washington, DC: Department of Defense.

Gates, R.M. (2008). *National Defense Strategy*. Washington, DC: Department of Defense.

Gates, R.M. (2009a). "Submitted Statement to Senate Armed Services Committee (January 27, 2009)." Washington, DC: U.S. Senate.

Gates, R.M. (2009b). *Quadrennial Roles and Missions Review Report*. Washington, DC: Department of Defense.

Gates, R.M. (2009c). Memorandum, June 23, 2009. "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations." Washington, DC: Department of Defense.

Geers, K. (2008). *Cyberspace and the Changing Nature of Warfare (IST-076/RSY-017)*. Tallinn: Cooperative Cyber Defence Centre of Excellence.

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.

Gorman, S. (2009). "Electricity Grid in U.S. Penetrated By Spies." *The Wall Street Journal*, April 8. Available from http://online.wsj.com [Accessed May 3, 2009].

Governors Highway Safety Association. (2009). "Cell Phone Driving Laws." Available from http://www.ghsa.org [Accessed April 1, 2009].

Hamill, S.D. (2009). "Students Sue Prosecutor in Cellphone Photos Case." *New York Times*, March 26. Available from http://www.nytimes.com [Accessed March 30, 2009].

Housman, R. (2009). "The Cyber Secure Institute." *Homeland Defense Journal*, 6(7), 17.

Hughes, R.B. (2009). "NATO and Cyber Defence: Mission Accomplished?" *Atlantisch Perspectief*, 1, 4–8.

Internet World Stats. *Top 20 Countries with the Highest Number of Internet Users*. Available from http://www.internetworldstats.com [Accessed March 31, 2009].

Lake, B. (2009). CyberThreats: A Cultural Change of Combating Threats. *Homeland Defense Journal*, 6(7), 14–16.

Langevin, J.R. et al. (2008). *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies.

London, England Hacker Indicted Under Computer Fraud and Abuse Act for Accessing Military Computers, 2009. Washington: Department of Justice. Available from http://cybercrime.gov/mckinnonIndict.htm [Accessed March 24, 2009].

McAfee. (2009). *Unsecured Economies: Protecting Vital Information*. Santa Clara, CA: McAfee

National Institute on Deafness and Other Communication Disorders. (2007). *Cochlear Implants*. Available from: http://www.nidcd.nih.gov/health/hearing [Accessed April 1, 2009].

Obama, B.H. (2009). *Remarks by the President on Securing Our Nation's Cyber Infrastructure*. Washington, DC: White House.

Optobionics. (2008). *ASR Device*. Available from http://www.optobionics.com [Accessed April 1, 2009].

Richardson, R. (2008). *CSI Computer Crime & Security Survey*. Computer Security Institute.

Rotenberg, M. & Laurant, C. (2005). "EPIC Statement on COE Cybercrime Convention, Treaty 108-11." Letter to Senators Lugar and Bidden, July 26, 2005.

Rumsfeld, D.H. (2003). *Transformation Planning Guidance*. Washington, DC: Department of Defense.

Rumsfeld, D.H. (2006). *Quadrennial Defense Review Report*. Washington, DC: Department of Defense.

Sang-Hun, C. & Markoff, J. (2009). "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea." *The New York Times*, July 10. Available from http://www.nytimes.com [Accessed July 14, 2009].

Schifferes, S. (2008). "Internet Key to Obama Victories." BBC News. Available from http://newsvote.bbc.co.uk/ [Accessed April 1, 2009].

Sharp, W.G. Sr. (1999). *CyberSpace and the Use of Force*. Falls Church, VA: Aegis Research.

Starner, T. & Paradiso, J.A. (2004). Human Generated Power for Mobile Electronics.

U.N. News. (2008a). "UN Forum Tackles Balance Between Property Rights and Internet Freedom." Available from http://www.un.org/news/ [Accessed March 30, 2009].

U.N. News. (2008b). "UN Forum Wraps Up With Call for Collaboration to Achieve 'Internet for All.' " Available from http://www.un.org/news/ [Accessed March 30, 2009].

U.S. Department of Energy. (2007). "Experiment Showed Grid Vulnerability to Cyber Attack—Flaws Fixed." *Energy Assurance Daily*, September 27. Available from http://www.oe.netl.doe.gov/ [Accessed May 7, 2009].

U.S. Department of Justice. (2009). *Computer Crime Cases*. Washington, DC: Department of Justice. Available from http://www.cybercrime.gov/cccases.html [Accessed March 24, 2009]

U.S. Government Accountability Office. (2008). *Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise (GAO-08-825)*. Washington, DC: Government Accountability Office.

Varnado, S.G. (2005). *SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems*. Washington, DC: U.S. House of Representatives.

Wilson, C. (2008). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (CRS Report for Congress RL-32114)*. Washington, DC: Congressional Research Service.

Woolley, P.L. (2006). *Defining Cyberspace as a United States Air Force Mission*. Master's Thesis, Air Force Institute of Technology.

Essay 12

Effects-Linked Comprehensive Planning
Integrating Military Planning with Interagency Implementation

By Jon W. Stull

Abstract

Despite expectations of a "New World Order" at the close of the 20th century and the potential for transformational innovation in the current century, the challenge of responding to international crises, and specifically complex contingencies, persists. Rapidly changing global environments, coupled with technological advances, require large institutions to significantly change their approach to solving complex new problem sets by transforming their organizations and processes. Both the U.S. Department of Defense and the U.S. Department of State worked to transform their institutions to achieve tighter integration of their respective efforts and those of other agencies to conduct complex operations abroad, especially reconstruction and stabilization. Despite significant progress in establishing a comprehensive, whole-of-government approach in implementing national policy, there remains the sense that the two major players are operating in parallel, not intersecting or integrating their planning efforts. As the military and diplomatic communities revise and refine the manner in which they plan, they have developed procedures that are asynchronous and difficult to integrate. However, embedded within recent initiatives are linkages that can assist whole-of-government and military planners to improve comprehensive approaches to more effectively deal with challenges of bringing failed or failing nations back into the fold of functioning global community.

229

Introduction

The last century closed with the unfilled promise of a "New World Order," and the new century has extended opportunity—and confusion—with the nexus of globalization and the rise of the Information Age. This dynamic of undefined and rapidly changing global environments, coupled with technological advances, has required large institutions to significantly change their approach to solving complex, new problem sets by transforming their organizations and processes. Seven years ago, the president of the United States challenged the nation to "transform America's national security institutions to meet the challenges and opportunities of the twenty-first century" (Office of the President of the United States, 2002, 2), and later charged national security institutions to "[improve] the capacity of agencies to plan, prepare, coordinate, integrate, and execute responses covering the full range of crisis contingencies and long-term challenges" (NSS, 2006, 45). To that end both the Defense Department and the State Department worked to transform their institutions for tighter integration of their efforts and those of other agencies to conduct complex operations abroad, especially reconstruction and stabilization. President Obama has continued and renewed the drive to "strengthen interagency coordination" and "ensure seamless integration" of interagency coordination (Presidential Study Directive 1, February 23, 2009).

Despite significant progress in designing organizations and processes to establish a comprehensive, whole-of-government approach to implementing national policy, there remains the sense that the two major players, Defense and State, are operating in parallel but are not intersecting or integrating their planning efforts. As the military and diplomatic communities revise and refine the manner in which they plan, they have continued to develop procedures that are asynchronous and difficult to integrate, resulting in waste and duplication while delaying desired effect and effectiveness. A military commander will likely analyze the operating environment and conceptualize lines of operation (LOOs) and decisive points in a concept plan well before the Country Reconstruction and Stabilization Group (National Security Presidential Decision 44, December 2006) proposes a policy planning template for reconstruction and stabilization (U.S. Joint Forces Command, 2005, 21). This essay discusses how to glean appropriate

guidance from national strategy or international mandate so that implementation can be integrated in a comprehensive manner, thus establishing "sufficiency-of-government" (C. J. Cunningham, personal communication, February 19, 2009) that can couple with other enablers to more effectively deal with challenges of bringing failed or failing nations back into the fold of functioning global community.

What makes complex operations, emergencies, or contingencies complex? Many situations to which the world community is expected to respond are complex because they share three basic characteristics. First, the requirement is time-sensitive, thus necessitating an immediate or near-immediate response. Second, the nature of the exigency requires response from several agencies or departments, not just the State Department and the U.S. Embassy, and not just Department of Defense organizations and commands. This leads to a third factor: security. Because of security concerns in any given scenario, a significant player in complex contingencies will be a uniformed military presence, both for security and for support in alleviating the suffering. This is evident in many natural disasters, where the effect of natural or manmade events far exceeds the capabilities of the affected nation, or in the wake of war or widespread hostilities, where reconstruction efforts and stabilization operations are needed to prevent further deterioration of government or infrastructure. Integrating the activities of several U.S. Government agencies within the comprehensive planning effort typical of military operations has been confounded by differences in organizational structure and culture, planning processes, and capabilities.

A Persistent Challenge

Lack of order following regime change has consistently been identified as a major challenge in the wake of operations *Just Cause* in Panama, *Provide Hope* humanitarian intervention in Somalia, and *Uphold Democracy* in Haiti, and most recently in Afghanistan and Iraq during operations *Enduring Freedom* and *Iraqi Freedom*. Repeated lessons were identified, focusing on the lack of order after regime change had occurred. Despite efforts, some significant, by many planners in several agencies (most notably the Departments of Defense and State) over the last two decades, the U.S. national response to complex contingencies continues to be marked by a lack of coordinated, integrated planning and execution that hinders progress

and aggravates cost. These deficiencies are manifest in inefficient or duplicative use of funds, inconsistent or insufficient allocation of manpower, decreased progress or effect in the affected country, and ultimately loss of national stature.

Can this persistent challenge be mitigated? Much discussion, some analysis, and steadily increasing awareness of need within the primary agencies involved led to some increase in the presence, and hence potential integration, of senior staff planners into the Department of Defense senior-level schools. Likewise, the Department of Defense has increased its presence in many Foreign Service Institute courses, and has increased its presence on Department of State staffs. In some focused activities, such as in the Office of the Coordinator for Reconstruction and Stabilization, collaboration may even be said to have increased significantly.

Two factors reduce the effectiveness of these efforts. First, the State Department and other non–Department of Defense departments and agencies have historically not been resourced (personnel and money) for such "educational" commitments and are reluctant to divert resources from statutory mission requirements to educating employees. Second, senior service schools and the Foreign Service Institute tend to address the challenge of developing a comprehensive approach to implementing policy at the strategic level of planning. Lack of participation and failure to focus on coordination at the operational level of planning will continue to plague U.S. national planning, and practitioners will thus fail to address or solve shortcomings.

Even if the resource issues were resolved, an operational disconnect will persist because various department and agency planning efforts run near simultaneously and in parallel, with no formal intersection or nexus. In reviewing the lessons identified from operations such as those mentioned above, it was failure to coordinate the actions of planners at the operational level, not the strategic level, that has resulted in delayed or inefficient application of national assets in resolving crises (Hayes & Wheatley, 1996). Therefore, this integrated planning dilemma is not ultimately a resource issue (although increased resources for civilian engagement in whole-of-government contingency planning would be most constructive).

A transformation of agency resourcing and organization is required to address problems from a whole-of-government or comprehensive perspective, including how agencies process, coordinate, and share information to "operationalize" a strategy, not just establish policy.

Most difficult of all, it will be necessary for large bureaucracies and organizations to influence their respective cultures to adopt and value the nature of proposed changes toward whole-of-government planning for response to complex contingencies.

Complex Contingency Operations

What are these complex contingencies? The term "complex contingencies" and its associated term "complex emergencies" (Bennett, 2002, 9) have been used to refer to those national and international operations that address significant humanitarian assistance to mitigate suffering and hasten recovery from natural disasters such as earthquakes, severe flooding, drought, and crop failure or from man-made exigencies generated from civil war, ethnic cleansing, and other government failures that create significant numbers of displaced personnel and refugees. The nature of these operations requires great effort for humanitarian relief and disaster assistance and, additionally, a significant presence of military (Chairman of the Joint Chiefs of Staff, 2001, 86). This military presence is intended not only to bring unique capabilities to support the humanitarian aspects of the operation but also to maintain order and establish security to enable effective relief, as well as to discourage exploitation of the crisis by dissident factions' efforts. Many times the security requirement exists as a result of natural disaster, as in response to earthquakes or flooding where looting or individual quests for food and water make areas unstable. Military presence, if immediate, can effectively counter the impromptu deterioration in civil order. Of much more challenging nature are those emergencies caused by political displacement of populations. Regime change, civil war, peacekeeping operations, and population migrations establish a need for a more persistent and comprehensive military presence. It is during these latter operations that the tasks required during complex contingencies, mentioned earlier, merge with the types of activities associated with the current term "reconstruction and stabilization."

Military Process and the Operational Continuum

For either of the operations mentioned earlier—military support for complex contingencies or emergencies—military planners will generally conceptualize and initiate planning in a manner similar to that used in anticipation of major combat operations. Most U.S. military

planning is done within the Joint Operations Planning and Execution System, which is now rapidly evolving as the Adaptive Planning and Execution System (Chairman of the Joint Chiefs of Staff, 2006a). The decision-making process resident within this system is the Joint Operating Planning Process. Regardless of how one views the overall military planning system, this decision-making process is certainly not unique to joint operations (operations that include military services from more than one department, e.g., both Army and Air Force). Each of the military services and many multinational partners have similar planning systems, as do some large corporate entities. Presented a problem or dilemma, most successful organizations will define the problem, assess the operating environment and factors bearing on the problem, propose options, analyze the potential benefits and risks of each of the options, recommend the option to implement, and submit a plan for implementation of the selected recommended option. Although most agencies and organizations conduct their decision-making along similar methods, it is the analysis of the problem and the design of the proposed solution that warrant a more detailed examination and that could be the nexus of planning, not just among militaries but across governments and multinational organizations.

Designing LOOs to Unhinge a COG

Given a task to accomplish (or support to be rendered), most militaries will initiate a period of assessment and analysis in which the nature of the task is clearly defined, the complex nature of the operating environment is thoroughly examined, and contributing factors that must be addressed to effectively accomplish the task are identified. Military planners call this initial examination "mission analysis" (Chairman of the Joint Chiefs of Staff, 2007, III-20-21). In large and complex operations against a significant threat or declared enemy, the military will examine critical factors and attempt to identify a "center of gravity," or COG (Joint Chiefs of Staff, 2007, IV-8) of the adversary, which, if attacked, can cause significant dislocation of the adversary's ability to continue to operate. Once a COG is identified, then operations are designed to bring international or national elements of power to bear on unhinging the enemy from the COG. Because most COGs are not exposed or vulnerable to our initial operations, other subordinate/intermediate objectives need to be identified with appropriate plans to muster assets, establish constraints, and provide

restraints to create desired conditions within the operating environment or modify the behavior of belligerents. Those subordinate/intermediate objectives are determined by analyzing the critical factors of the adversary or hostile environment and then determining which decisive points (Joint Chiefs of Staff, 2007, IV-16) should be achieved to exploit critical vulnerabilities, which may in turn expose the COG. In determining what constitutes a decisive point, the commander and his staff will identify what conditions need to exist to achieve the strategic/operational objective and what accomplishments are necessary to effect achieving the main (strategic/operational) objective. Attaining or seizing each of the intermediate objectives (which have been identified earlier as decisive points) will establish conditions and effects that are necessary to achieve subsequent operations and reduction of the COG. The connecting of these decisive points thus becomes what is known as a LOO (depicted in figure 1, as a modified version of figure 4 from doctrine on Joint Operation Planning; Chairman of the Joint Chiefs of Staff, 2006b, IV-12-13).
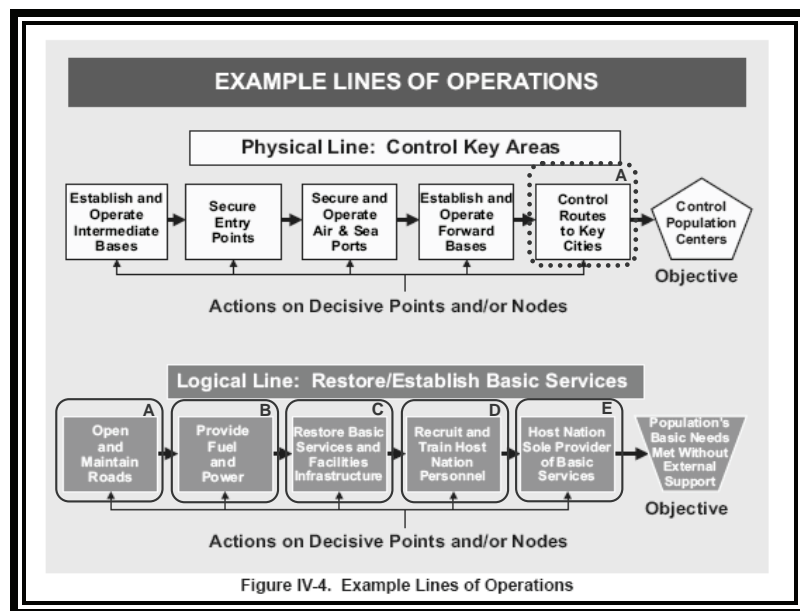

Figure IV-4. Example Lines of Operations

Figure 1: Lines of Operation With Author's Annotation (Red). (Source: Chairman of the Joint Chiefs of Staff, 2006b, IV-13)

A commander of any major operation will develop any number of LOOs and control numerous decisive points in an effort to affect the

adversary's COG. These LOOs may be strictly geographic features or key physical points, as depicted in a physical LOO, or may be more focused on functions and conditions, as illustrated by a logical LOO. It is likely in any given major operation or campaign that a commander may design a combination of both physical and logical LOOs. It is this analysis for designing a campaign or a major operation that is known as operational art and is the realm of the major military commands and of the U.S. Combatant Commanders. The exercise of operational art and the design of a major operation, whether it is combat or military support to other agencies or organizations, does not occur within a single military or physical dimension.

Today's operating environment is increasingly complex. That complexity is magnified in complex contingency operations because of the diversity various players and components bring to the operation. Achieving an objective within one aspect of the operating environment will likely have an effect or create an effect in another aspect. When the military commander destroys a bridge to deny exposure of his flank to the enemy, this action initially appears to support a legitimate military objective. If the consequence or effect of destroying the bridge results in the inability of the local population to conduct trade and support their families, leading to local frustration, unemployment, and social unrest, local election results might be influenced so that a regime predisposed to achieving desired original policy goals fails to come to power. This failure is inconsistent with an original, more important, and broader mission of stabilizing the region.

Interconnected Complex Environments

Breaking down the complex operating environment into various generic systems helps to envision the potential interconnectedness of the operational environment. Present joint doctrine identifies the possible systems within a complex operating environment as political, military, economic, social, information, and infrastructure (Chairman of the Joint Chiefs of Staff, 2006b, IV-4–5). The example above of the destruction of a bridge clearly illustrates how an action within the military arena could affect transportation infrastructure, which aggravates poor economic conditions, which may, in turn, generate social dissatisfaction and influence desired political end states.
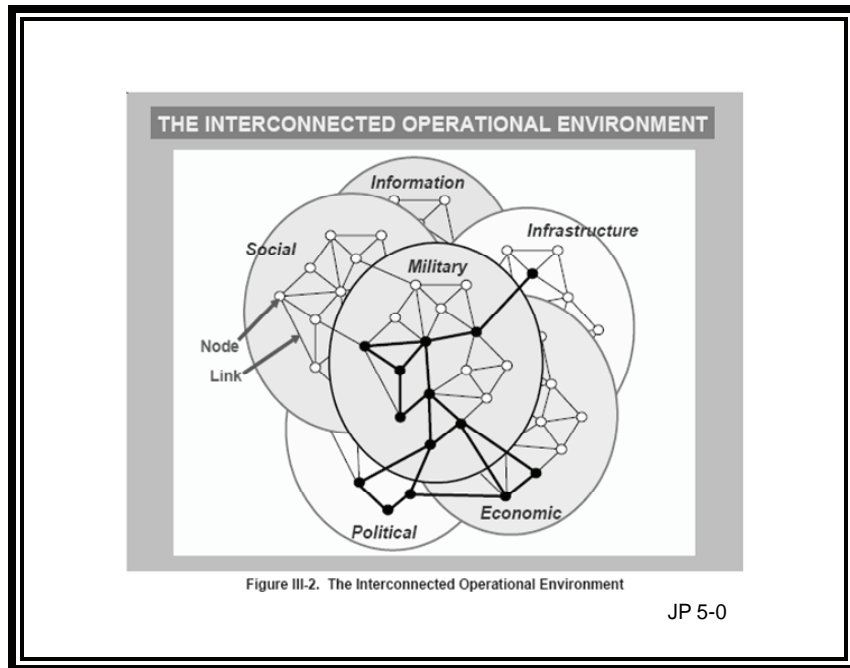
Figure III-2. The Interconnected Operational Environment

JP 5-0

Figure 2: The Interconnected Operational Environment (Source: Chairman of the Joint Chiefs of Staff, 2006b, IV-5)

This is not to say that each decisive point achieved or objective taken generates effects that can be extended out to other systems with certainty. However, this does suggest that the operational environment for complex contingencies and stabilization operations, where many agencies can exert elements of national and international power, is an environment in which one agency's actions can establish a condition, intended or unintended, that may affect other activities or systems, and consequently the actions, outcomes, and effectiveness of other agencies.

This operational level of planning is not unique to the military but is resident in some large corporations and bureaucracies as well. Whenever there is a level of planners who must interpret a strategy, issue guidance, and provide resources to a subordinate level of planners (who are then responsible to execute the operation), you have established an operational level. To "operationalize" a policy or a task established by higher authority means that the operational-level planner

must define the task so it can be understood and quantified by those who will carry it out. In addition, in doing so, the operational-level planner needs to scope the problem establishing limitations and identifying resources to be used. If the subordinate organization, which is to execute the task, needs support from outside their organization, then that too must be identified, and how that supporting relationship is to be managed must be described. In addition, and critical to the success of achieving the mission, performance measurements or metrics (U.S. Joint Forces Command, 2005, 21) must be identified to determine progress and ultimately success. This interpretive level of giving planning substance to relatively broad, if not vague, strategic visions for subordinate levels to execute is the guts of what is expected at the operational level. Although this process is carried out in most departments and agencies, it is normally done within the agency and has not, in the past, been structured to be done in a comprehensive manner across agency or department organizational boundaries at an operational level of planning.

Transforming Interagency Coordination

A comprehensive review of the many departments and agencies that are involved in complex operations is well beyond the scope of this article. An examination of the political and military departments that are or should be at the center of whole-of-government solutions illustrates the challenges in coordinating a comprehensive approach to complex operations. There have been several recent initiatives that, if considered by the Obama administration, will be able to give a solid foundation for further transformation in planning whole-of-government approaches to policy implementation. In the wake of the U.S. experience in Somalia 1992–93, followed closely by involvement in Haiti in 1994–96 and continuing challenges in the Balkans, both civilian and military planners created a format for a generic political–military plan in responding to complex contingencies. In May 1997, the Clinton administration promulgated Presidential Decision Directive 56, Managing Complex Contingency Operations. This document directed and required a political–military implementation plan that would "outline an integrated concept of operations to synchronize agency efforts" (Presidential Decision Directive 56, 1997) This initiative to establish an acceptable interagency method for improving the planning process was followed by the Bush administration's desire to establish

organizational structure that may better enable an integrated agency approach to planning. On December 7, 2005, National Security Presidential Directive 44, Management of Interagency Efforts Concerning Reconstruction and Stabilization, was issued by the Bush administration. This directive established an interagency entity within the State Department known as the Office of the Coordinator for Reconstruction and Stabilization for the purpose of integrating the efforts of U.S. Government agencies, as well as harmonizing government efforts with those of the military (National Security Presidential Directive National Security Presidential Directive 44, 2005).

Once established, the Office of the Coordinator for Reconstruction and Stabilization, in coordination with the Department of Defense, and more specifically the U.S. Joint Forces Command, collaborated in developing the U.S. Government's Draft Planning Framework for Reconstruction, Stabilization, and Conflict Transformation (U.S. Joint Forces Command, 2005). This planning framework was instrumental in establishing a planning process and, in short, effecting a strategy with which to operationalize policy. Historically, policy, once stated, was forwarded to the various departments and agencies in the field for implementation, with the lone coordinator for interagency integration being the ambassador and the country team. This was insufficient to effectively implement policy that should be expeditiously resourced and assessed. Based on experience gained from U.S. involvement in international efforts to relieve complex emergencies in the Balkans, a forerunner of this planning framework was noted by Len Hawley in his discussion of "advance political-military planning" with the aim to "harmonize the many diverse civilian and military efforts as a comprehensive strategy" (Covey et al., 2005, 37–76). The establishment of a structured planning process created a common planning document that permitted various agencies and departments of the government to integrate their respective efforts and harmonize civilian activities with those of the military. The framework details a process that calls for interagency participation in the formulation of an overall policy goal stated as an outcome (U.S. Joint Forces Command, 2005, 21). Although talented and well-meaning players from all departments and agencies would do their best to coordinate "on the ground" once face-to-face, this proved to be insufficient, time-consuming, and wasteful of limited resources. To mitigate the challenges of operationalizing policy, the Draft Planning Framework

(U.S. Joint Forces Command, 2005, 14) defines a strategic level of the planning process in which major mission elements (MMEs) are identified. These MMEs are identified at the policy-making level and are large accomplishments that are individually necessary to achieve the overall goal, and which, taken together, are sufficient to reach the overall desired outcome of the policy. Once the overall policy goal and the required major outcomes (MMEs) to achieve the goal have been identified, the organizations and commands in the field establish sub-objectives and tasks that they can achieve that will, in turn, affect the desired outcome of respective MMEs. The overarching policy goal, the various major accomplishments (MMEs), and the sub-objectives and tasks necessary to attain the MMEs are all written as outcomes, not as tasks (U.S. Joint Forces Command, 2005, 21). A representative sample of this hierarchical format for strategic guidance is depicted in figure 3 and is based on the discussion generated for responding to a hypothetical complex contingency.
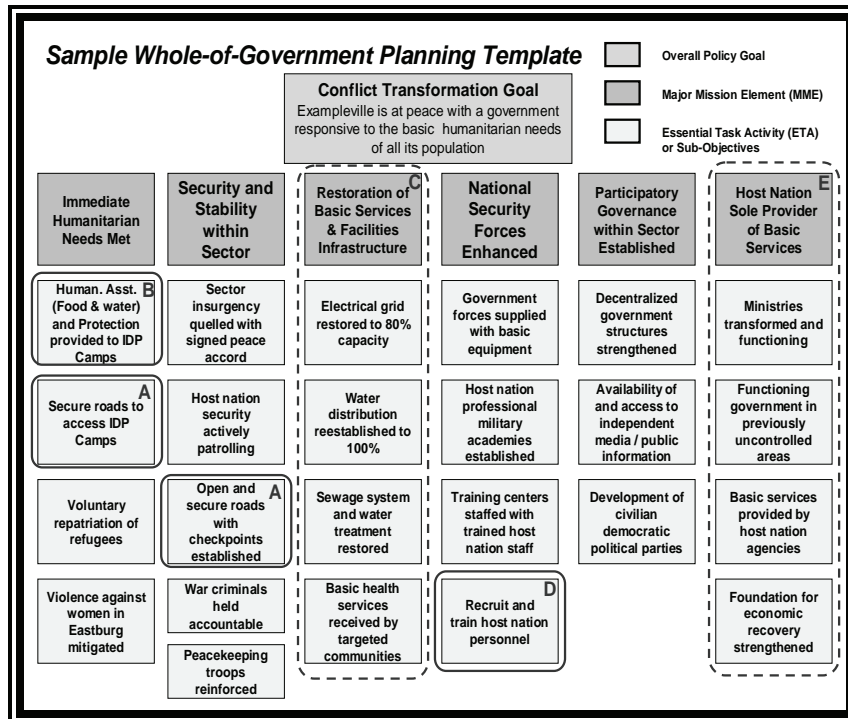

Figure 3: Annotated Extract of S/CRS Planning Template based on Sample Planning Template (USJFCOM, 2005, p.43).

Even with the initiation of a standardized transformation of the planning process for integrating multiple government agency planning activities, the capacity to harmonize similar efforts with the potentially substantial footprint of the military remained problematic. For the U.S. Government, policy formulation is done at the highest strategic level within the National Security Council structure. Once determined, the operationalizing of that policy is forwarded to the field or the ambassadors and their country teams to coordinate the implementation of that policy. Harmonization of efforts with the military was then done at the field implementation level with the country team. However, as stated earlier, many of the operational-level decisions for the military are made by the theater or unified commanders at a distinct operational level of planning.

To mitigate this disconnect between nonmilitary and military planning, in the National Military Strategy (2004, 21), the Department of Defense established Joint Interagency Coordination Groups at most of the unified commands in an effort to improve cross-agency coordination and sharing of information. This originally was instituted with a focus on countering terrorism and has since evolved to encompass most military operations that have other agency or international participation. This structure, however, was not universally accepted by the various unified commanders' planning staffs and encountered significant difficulty being staffed by several agencies from outside the Department of Defense. Accordingly, the ability to coordinate planning at the operational level was never optimized.

To remedy this gap at the operational level of planning, the National Security Council Reconstruction and Stabilization Policy Coordination Committee published a concept (National Security Council, 2007) to establish an Interagency Management System for Reconstruction and Stabilization that would augment field planners at the embassy and fill the gap for coordination with the unified commanders at the operational level of planning. Once activated, the Interagency Management System would establish a Country Reconstruction and Stabilization Group to conduct detailed strategic level planning, and augment embassy country teams with advance civilian teams to assist in comprehensive integration at the implementation level, as well as field advance civilian teams that would displace forward into regions to conduct the implementation of the policy. At the operational level, where previously no one other than a major military command would be coordinating or planning, an integration planning cell was designed "to

support integration of civilian and military planning at a GCC, or at an equivalent multi-national headquarters" (National Security Council, 2007, 11). However, even with the establishment of a transformed process and newly established innovations for organizations, comprehensive planning efforts are still likely to be parallel efforts that find integration difficult.
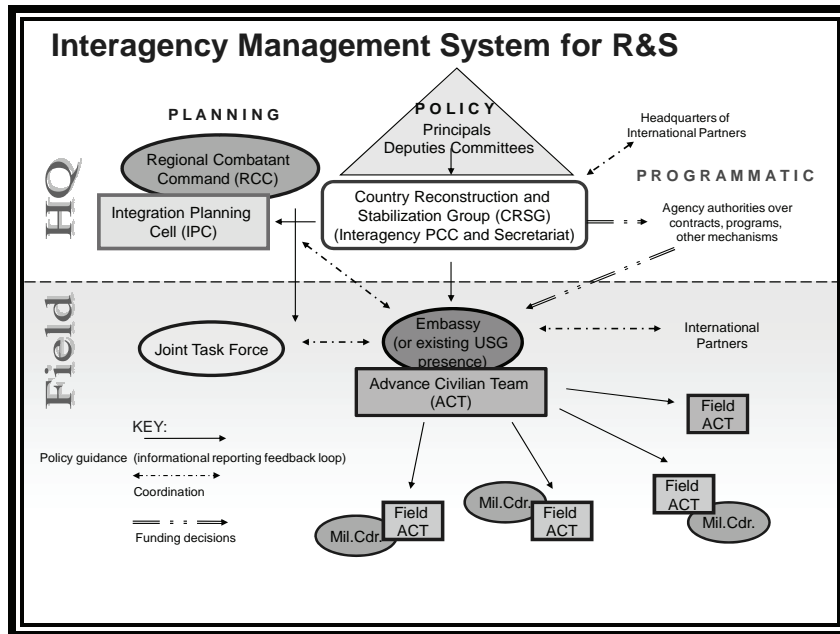

Figure 4: Interagency Management System (Source: NSC, 2007, 3)

The Nexus of Cross-Department/Agency Planning

Operational level planners, regardless of department or agency, whether civilian or military, design their operations in similar yet not identical manners. This level of planning should focus on where the different systems intersect to integrate or harmonize a comprehensive, whole-of-government approach to implement policy. Present initiatives affecting the two main entities of military and policy planners have established conditions favorable to this nexus of strategic guidance and operational planning. As previously discussed, military planners anticipate requirements and construct possible concept plans for the use of significant military resources. In designing these operations,

planners identify decisive points and intermediate objectives that must be achieved to accomplish the mission. The planner will postulate what conditions are required to achieve the objectives. Thorough analysis by military planners reveals that achievement of these decisive points and the taking of intermediate objectives will require either that certain conditions be established beforehand or that certain effects will be generated as a consequence. The example identified earlier in figure 1 showed both physical and logical LOOs. At times, achievement of decisive points or sub-objectives in one LOO will be similar, if not identical, to conditions created by another LOO. Take the example of actions on decisive point marked "A" and circled with a dashed line on the physical LOO ("Control Key Routes to Key Cities") and compare it with decisive point "A" circled with a solid line on the logical LOO ("Open and Maintain Roads"). Although not identical, a commander, if using both these lines of operation, will find a point of intersection at those respective decisive points that will require close integration.

Civilian policy planners, as discussed earlier, draft overarching policy goals, major mission elements, and sub-objectives or essential task activities, which are articulated as outcomes. Outcome language of the proposed U.S. Government Draft Planning Framework stipulates the specific condition or consequent effect of actions taken so that progress can be measured. The articulation by civilian policy planners of various outcomes and effects to be attained as policy goals or major mission elements will be stated in a similar manner to those of military planners, who articulate the effects or conditions that may be achieved as a result of taking intermediate objectives and decisive points. The language in these two different planning documents will be so similar at some points that it will be evident that the language identifies the same condition or effect in each of the documents. Extending the example of the military commander, offered earlier, who has identified the criticality of "controlling key routes" and "opening main roads" (decisive points "A"), intersection with outcomes identified in the Office of the Coordinator for Reconstruction and Stabilization Planning Template (figure 3) is apparent. A basic examination of the planning template at figure 3 shows clear points of intersection with the military commander's previous analysis of decisive points in designing lines of operation. In figure 3, the lettered boxes identified in figure 1 have been overlaid onto the whole-of-government planning template. This clearly identifies actions that, at some decisive points that a military commander may deem appropriate, will affect—if not lead to—

outcomes identified in a comprehensive policy plan. If the military commander achieves actions circled as "A" in figure 1, then it is obvious it will affect, if not be essential to, achieving outcomes circled and identified as "A" in figure 3, the whole-of-government policy planning template. As further depicted by comparing actions identified in a military commander's lines of operation (figure 1) with the outcomes identified with the corresponding letters in the whole-of-government planning template (figure 4), some actions of a military commander are associated with sub-objectives or essential task activities in more than one major mission element (activities circled labeled "A"). Further, some actions identified by the military commander in designing a LOO may encompass a complete MME, as illustrated by both items labeled "C" and "E" in each of the figures ("Restoration of Basic Services . . . " and "Host Nation Sole Provider . . . "). It is at these points of congruence that military planners should identify and recommend what should be a defense lead in a whole-government or comprehensive approach plan. By extension, this crosscutting technique will not only identify what outcomes should be identified as having the military take the lead responsibility but also will identify conditions that the military will achieve that will support another government agency or department. This technique forces the two major parallel planning efforts of the primary players in a whole-of-government approach policy implementation to intersect. It is at this intersection, or the nexus of these two major planning efforts, that planners must focus to ensure that efforts across government (or international organizations in the case of multinational operations) are brought together to establish a coherent application across the spectrum of elements of power assembled for any particular contingency.

Conclusion

Although the drive for transformation in government has initiated some significant innovations in both organization and process, these efforts are nascent, and their effects remain unfelt by the majority of the vast complex operations planning and execution community. To move from the conceptualization of improving comprehensive integration of national and international elements of power or influence to application, points of intersection must be identified. Overlaying a military commander's operational design, which likely has been prescribed in an earlier draft concept or operations plan, with a more

recently developed planning template drafted by the strategic-level planners, points of intersection can be identified by pairing up the military commander's decisive points and the effects intended to achieve those objectives with the MMEs and the sub-objectives or essential task activities that are written as outcomes. Activities or elements for which the military should take the lead, when identified in the language of military effects gained through decisive points in the plan's various LOOs, will be almost identical to the outcome language of properly articulated MMEs and essential task activities of the interagency implementation plan/planning framework. This is not a call to revert to an effects-based approach to operations, but, rather, a realization that in executing objectives-based operation plans, military commanders will affect conditions needed in achieving the whole-of-government comprehensive plan, thus demonstrating that military plans and comprehensive government plans are "effects-linked." The diplomatic and military communities can no longer afford to conduct their respective detailed planning in parallel; they must drive their respective efforts to a point of nexus or intersection to mitigate the fog of complex operations: "Who's responsible for what, and who will resource which activity?"

Schools, academies, and training centers should practice this intersection of political and military planning, so that theory can be taken out of the classroom and applied in the field. Efficiencies of proper strategic-level and operational-level planning must be realized. The rudiments of a transformed planning process and the basis for transformed organizations to exercise this process are present and must be used every time exercises are planned or policy is considered for implementation. This will require military contingency planning, to begin with the end in mind and identify effects or conditions that will be required in the later phases of an operation (i.e., stabilization and enabling civil authorities). Only after identifying where the plan must take them should military planners then design how the earlier phases of the plan frame deterrence, seize initiative, and generate dominating actions. There should be no detailed planning of dominating activities before the stabilization activities and the actions that enable civil authorities have been identified and all parties have analyzed how their respective plans are "effects-linked."

This will not be accomplished without challenges. The timing of these respective planning communities is not concurrent. Military planners will likely have their rudimentary operational design and

concept plan "on the shelf" before the strategic planning team of the Country Reconstruction Stabilization Group have even convened. Accordingly, civilian planners need to avail themselves of previously documented military plans, and defense establishments need to ensure permission so that those plans can be shared outside of the defense establishment. In addition, those who develop strategic plans that include proposed outcomes must be open to input, feedback, and proposed adjustments of those who will implement the plan.

The world community will continue to experience challenges created by natural or manmade disasters. Whether they are called "complex contingency," "reconstruction and stabilization," or "stability" operations, multinational and/or national planning efforts must become more effective, and thus more efficient. This can be advanced significantly if both military and civilian planners seek integration at points of intersection of their respective planning efforts where they are obviously "effects-linked."

References

Bennett, C. (2002). *Office for the Coordination of Humanitarian (OCHA) Affairs Orientation Handbook on Complex Emergencies*. New York: United Nations.

Chairman of the Joint Chiefs of Staff. (2001). *Joint Publication 1-02 (JP 1-02), Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2004). *National Military Strategy (NMS) of the United States of America*. Washington, DC: Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2006a). *Joint Operation Planning and Execution System (JOPES) Volume I, Planning Policies and Procedures*. Manual 3122.01A, September 29, 2006. Washington, DC: Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2006b). *Joint Publication 3-0 (JP 3-0), Joint Operations*. Washington, DC: Government Printing Office.

Chairman of the Joint Chiefs of Staff. (2007). *Joint Publication 5-0 (JP 5-0), Joint Operation Planning*. Washington, DC: Government Printing Office.

Covey J. et al., eds. (2005). *The Quest for Viable Peace.* Washington, DC: Institute of Peace Press.

Hayes, M.D. & Wheatley, G.F. (1996). *Interagency and Political-Military Dimensions of Peace Operations: Haiti: A Case Study*. Washington, DC: National Defense University.

National Security Council. (2007). Reconstruction & Stabilization Policy Coordination Committee approved white paper. *Interagency Management System for Reconstruction and Stabilization*.

Office of the President of the United States. (1997). Presidential Decision Directive 56/National Security Council white paper. *Managing Complex Contingency Operations*.

Office of the President of the United States. (2002). *The National Security Strategy of the United States*. Washington, DC:.

Office of the President of the United States. (2005). National Security Presidential Directive 44. *Management of Interagency Efforts Concerning Reconstruction and Stabilization (NSPD-44)*.

Office of the President of the United States. (2009). Presidential Study Directive 1. *Organizing for Homeland Security and Counterterrorism*.

U.S. Joint Forces Command. (2005). J7 Pamphlet Version 1.0. U.S. Government Draft Planning Framework for Reconstruction, Stabilization, and Conflict Transformation.

Adaptive Organizations

Maintaining Competitive Advantage by Exploiting Change

By Scott Moreland and Scott Jasper

Abstract

Information Age organizations are complex and dynamic "living" entities that interact with and influence their environments. People are the building blocks—creative and intelligent components with a latent ability to produce not only stipulated outcomes but also novel ideas and achievements. This realization is a dramatic departure from the traditional conceptualization of organizations as mindless machines that churn out prescribed, formulaic products and solutions in an industrial fashion. When visualized and treated as living systems, organizations more readily exploit emergent technologies, as well as the human potential to innovate and adapt. To realize their full potential, adaptive organizations must also be capable of managing and even encouraging disruptive change.

Adaptive organizations possess markedly cooperative characteristics that operate on trust, open information flow, and responsiveness to technological innovation. They are not based on or hostage to a set of inviolate roles, policies, and structures that form the rigid pillars for success. Rather, they purposefully reconfigure these important organizational components to support each new project or activity. Business models are changed as necessary.

Organizational transformation requires deep understanding of the operational environment, ability to shape structure and processes to perform optimally, and rapid action to exploit opportunities to exert influence and maintain competitive advantage. Actions are followed by careful evaluation of outcomes, which in turn leads to new understanding and subsequent adaptations. This may be codified into a continuous process: understand → shape → act → evaluate. This essay will also provide tangible evidence of how this process can facilitate rapid organizational assimilation of new technology and people innovations.

Introduction

Jingshen is the Mandarin word for spirit and vivacity. It is an important word for those who would lead, because above all things, spirit and vivacity set effective organizations apart from those that will decline and die.[1]

Modern organizations must be prepared to operate in a dynamic, information-saturated environment with increasingly porous boundaries. Ideas, creativity, and information services are the highly marketable commodities of the moment. Whole business entities have vacated their brick and mortar confines to float freely in the ether of cyberspace. Perhaps the most encouraging trend is the enhanced virtual interaction and collaboration among organizations, their people, and the recipients of the organization's product or service.

Technological innovations such as the Internet and satellite communications have fundamentally altered how organizations must relate to their stakeholders and the ambient environment in which they operate. In the commercial sector, companies like Amazon, Priceline, and eBay stake their entire business model on active consumer participation and feedback. These cyber-middlemen have resurrected barter commerce. They provide powerful tools for collaboration such as prominently posted reviews, product blogs and discussion, and facilitated correspondence and transactions between vendors and end-users. Even traditionally autocratic and highly structured defense organizations are incrementally implementing fundamental organizational changes such as decentralization and network centricity. Military organizations are actively seeking innovative solutions from academia and industry, along with the pragmatic creativity of junior military leaders as they grapple with sophisticated and elusive adversaries.

Despite these changes, organizations remain functionally static. At a fundamental level, an organization provides a structured model for its constituent entities that establishes purpose, fends off aggressive competition, and passes knowledge between contemporaries and from generation to generation. Organizations do not fulfill these basic

---

[1] James L. Hayes, *Memos for Management: Leadership* (New York: AMACOM Books, 1983), 51.

functions differently today from how they have since early civilization. It is the form of the organization that is in a state of constant evolution—optimizing its component parts to best respond to the environmental conditions of the moment, girding to grapple with new and unfamiliar problems, and improving the ability to gather, understand, and communicate information. The simple fact that organizations are and have always been adaptive has long been a topic for popular discussion and philosophical and political debate. For at least the past 50 years, it also has been a field of deliberate scientific study that sees organizations as complex adaptive systems.

A complex adaptive system can be defined as an entity that "behaves/evolves according to three key principles: order is emergent as opposed to predetermined, the system's history is irreversible, and the system's future is often unpredictable."[2] Certainly, modern organizations neatly fit this definition. Human history drifts between periods of alternating stability and disruption, more or less neatly bracketed by historians into "eras," with each era building from its predecessor. At this macro-temporal level, organizations tend to evolve more radically during the chaotic periods between eras. The contemporary era is popularly conceived to be occupying a wildly entropic time-space between the end of the Industrial Age and the beginning of a new era, which has been more or less accurately described as the Information Age. Regardless of the moniker, nations at the forefront are exporting Industrial Era productivity to the developing world, with important implications for the future. In the lead countries that are shaping globalization, the focus has shifted from productivity to agility—efficiency is trumped by flexibility, generic mass-production by service specialization, and compliance by innovation.

That said, this shift is not unprecedented, as it pertains to the consideration of organizations as complex, adaptive systems. The fundamental difference between post-Industrialism and previous eras is that there is an opportunity to shape change deliberately rather than reactively. "Information Age" accurately describes our current cognitive space: We are able to develop a "deep" understanding of our environment through novel technologies that are already influencing changes in the way we think, organize, and interact. In fact, the relatively new treatment of organizations as living, evolving entities

---

[2]Kevin Dooley, "A Complex Adaptive Systems Model of Organizational Change," *Nonlinear Dynamics, Psychology, & Life Science*, 1999;1(1):69–97.

may already be passé. Rather than adapting in the random or reactive fashion of natural evolution, our potential for "deep understanding" may offer us opportunities to transform organizations proactively and shape our environment deliberately to maintain competitive advantage.

Eras of radical change are generally tied to a paradigm-altering cognitive breakthrough, either instigated or enabled by technological advances. The introduction of agriculture, the preservation of ideas in writing, the harnessing of energy to produce electricity, and most recently, the creation and occupation of cyberspace have fundamentally altered the whole of human civilization. To navigate the disruption zones that herald these eras of revolutionary change, organizations must rapidly adapt or face obsolescence and ultimate extinction.

Before the advent of agriculture, human society conformed to a natural evolutionary progression; that is, its organizations and their adaptations were shaped by the physical environment. Agriculture was the first meaningful effort undertaken by humans to fundamentally alter their environment in a deliberate fashion, based on a new understanding of how things naturally worked and, with a bit of ingenuity and technological know-how, could work better to suit human needs. Even so, it took thousands of years for hunter–gatherer societies to give way to agrarianism, and illiterate civilizations thrived for millennia after the first Sumerian marked cuneiform onto clay. These historical innovations, which form the very basis of the ultimate complex adaptive organization—modern global civilization—occurred over a vast expanse of time. In contrast, the last two centuries have known almost constant change. The dizzying pace of modern-era revolutions—accessible energy and instantaneous communication grids, ventures into outer space, the realization of cyberspace—has radically and perhaps irrevocably shaped the ambient environment through the creation and occupation of previously unreachable or even unfathomable domains. Not content with merely changing our environment, humans are now exploring ways to shape our very essence as human beings as we begin to understand and exploit genetics, artificial intelligence, and nanotechnologies.[3]

The implications for post-Industrial organizations are profound. The pace of radical change is widening the gap between technological

---

[3] U.S. Joint Forces Command, "The Joint Operating Environment 2008: Challenges and Implications for the Future Joint Force." Available at https://us.jfcom.mil/sites/J5/J59/default.aspx.

possibilities and the ability of organizations to assimilate technology responsibly, purposefully, and ethically. A proactive, nonsequential approach to organizational adaptation combines four essential cognitive capabilities:

Understand → Shape → Act → Evaluate

First, organizations must understand themselves, their competitors, and their operational space. To survive and thrive, they must use innovation and technological enablers to shape both internal structures and fluid environmental conditions to ideally suit an organizational purpose. This understanding and preparation of a favorable ambient setting enables organizations to act with clear purpose and evaluate the outcomes of their actions and to determine both the immediate and potential long-term effects that will affect future understanding, form, and action, and indeed might either confirm or refute the continued relevance of an organization's purpose.[4]

Understand: Attaining "Deep Knowledge"

Kill our worst ideas before they kill us.[5]

The first step in achieving deliberate and desirable organizational adaptation is to attain a holistic understanding, or "deep knowledge,"[6] of self, peers and competitors, and the environment. Deep knowledge requires a departure from traditional ideas about organizational purpose and management.

The first conceptual hurdle is the notion of replacing control with agility. Agility, in fact, is the "critical capability that organizations need to meet the challenges of complexity and uncertainty."[7] Deep knowledge is based, ironically, on the concession that being able to unerringly forecast, much less control, the future operational

---

[4] David C. Gompert, "Heads We Win: The Cognitive Side of Counter-Insurgency," RAND Counter-Insurgency Study Paper 1, prepared for the Office of the Secretary of Defense by the Rand National Defense Research Institute, Santa Monica (2007).

[5] Joseph M. Firestone, "Reducing Risk by Killing Your Worst Ideas," *Knowledge Management Consortium International,* 2004:6.

[6] Mark W. McElroy, "The New Knowledge Management," *Knowledge & Innovation: Journal of the KMCI*, 2000;1(1):43–67.

[7] David S. Alberts, "Agility, Focus, and Convergence: The Future of Command and Control," *The International C2 Journal,* 2007;1(1):3.

environment is impossible. This realization does not mean that organizations should not bother to build future strategies—quite the contrary. For adaptive organizations, future planning simply shifts from a focus on control to a posture of careful monitoring and agile response based on a range of potential future scenarios. Planning for plausible future scenarios, coupled with continuous feedback from environmental scanning, can enhance awareness and increase responsiveness in an uncertain environment.[8]

Over 30 years ago, Shell Oil Company was one of the early developers of a "flexible response" approach to operating in an uncertain future.[9] In the late 1960s, rampant nationalization of global oil reserves sparked a disruptive change in the supply-side dynamic. When the Organization of Petroleum Exporting Countries (OPEC) emerged on the global scene in 1960, Shell recognized that this shift in the control of oil supplies from private industry to state entities might significantly alter the standing set of objectives, incentives, and practices that formed the foundation of the enterprise. Shell projects that were based on previous industry forecasts were failing, and the company's strategic planners began to recognize that planning future projects that were aligned with a single future scenario on the basis of past precedent was an unacceptably risky endeavor. They looked to the then-groundbreaking work of open-systems theorists Daniel Katz and Robert Kahn,[10] who asserted that when faced with an uncertain future, it is important to first determine which variables remain predictable. Then, based on what can be accurately predicted, a few plausible scenarios might emerge for future planning.

After careful consideration of a short list of planning scenarios, Shell adapted their business model to accommodate this new-found understanding of how to mitigate risk in an uncertain future. Project designers considered how their efforts might support a broader range of

---

[8] Kees van der Heijden, *Scenarios: The Art of Strategic Conversation*, 2d ed. (West Sussex: John Wiley & Sons, 2005), 83–85.

[9] "Shell Global Scenarios to 2025," (The Hague: Royal Dutch Shell, Shell Group, 2005), 8.

[10] Daniel Katz and Robert Khan were pioneers of social-systems theory. One of their early texts, *The Social Psychology of Organizations* (West Sussex: John Wiley & Sons, 1978), first published in 1966 and revised in 1978, is fundamental reading for social-systems theorists. This observation and its influence on the oil industry in the 1970s are found on pages 130–131 of the 1978 edition.

future scenarios, emphasizing agile and responsive capabilities that could address not only the most likely futures but also the most dangerous scenarios. In the case of scenario development for the nationalization of oil supplies, Shell's planners used global demand as their predetermined, or predictable, variable. Because demand was unlikely to change, this increased the weight of the supply-side variables. Initially, the planning team also considered supply to be fairly stable and that the most likely outcome was that state-controlled supply points would continue to generate anticipated oil production outputs. They also, however, considered a most-dangerous scenario, in which a major producer state or collective might alter production for national or political purposes not directly related to economic gain. Shell planners considered this to be the crisis scenario, and their project development efforts were arranged to be responsive to both these and other plausible futures.

After Shell's project development was aligned to be responsive to multiple future scenarios, it became imperative to determine the key indicators that a particular future scenario was emerging, which would trigger subsequent decisions and resource commitments. For the Shell scenarios, one obviously critical indicator was a political event that might encourage negative changes in nationalized (mostly Arab) crude oil extraction and distribution. The continued expansion of OPEC throughout the 1960s and the nationalization of Libyan oil under President Muammar Kaddafi in 1969 were significant indicators of the increasing potential for a most dangerous scenario outcome. Shell braced for the storm just as the Yom Kippur War between Israel and its Arab neighbors erupted in 1973. By the time OPEC producers imposed their devastating embargoes against Israel's supporters in the war, Shell had already recognized the implications and rapidly reduced its Middle East commitments and reliance on OPEC-controlled supply lines. To do this, Shell invested heavily in liquefied natural gas, developed supertankers to minimize traffic to and from supply chokepoints in the Arabian Gulf, began diversifying its energy portfolio to include coal and nuclear power, and shifted exploration from the Arabian Peninsula to the North Sea.[11] Though hardly immune from the effects of the 1973 embargo, Shell's responsive shifts ensured that the company would be among those that would survive the resultant industry crunch.

---

[11] Royal Dutch Shell, "Shell Global Scenarios," 22–26, 68–71.

At the end of the Cold War two decades later, the United States military likewise found itself in a future-planning quandary. A European ground war or nuclear exchange with the Soviet Union had long been the myopic future planning priority. With the sudden dissolution of the Soviet Union in 1991 and the ascension of small and nonaligned nations into the nuclear family, not to mention the emergence of ideologically motivated transnational terrorist organizations on the global scene, future-conflict scenarios began to look far more messy and unpredictable.

The terrorist attacks of September 11, 2001, the most devastating attack on U.S. soil since Pearl Harbor, highlighted just how uncertain the present and future security environment had become. The potential list of external threats had dramatically expanded, and it was clear that any attempt to focus narrowly on a particular group of adversaries would result in catastrophic response capability shortfalls against unanticipated challenges. The defense community radically altered the threat-focused planning paradigm to be more capabilities-based in an effort to prepare agile and responsive forces that would be able to effectively counter a broad range of threats. Similar to the Shell planning model, capabilities-based planning addresses environmental uncertainty by considering a wide range of possible scenarios; it then generates capability requirements that are applicable and essential to success in all of the scenario conditions.[12]

Shape: Adapting Organizations for Uncertain Futures

> Organizational capabilities represent the last truly sustainable source of competitive advantage.[13]

For the U.S. Department of Defense, the conceptual shift to capabilities-based planning and an adaptive, agile posture compelled significant organizational changes. The development of a flexible capabilities-based force would demand organizations with a broad mission set, an inclusive and cooperative mentality, a willingness to accept calculated risks, and a painful divorce from platform-centric

---

[12] *Quadrennial Defense Review Report* (Washington, DC: U.S. Department of Defense, 2006), 59.

[13] David Nadler and Michael Tushman, *Competing by Design: The Power of Organizational Architecture* (New York: Oxford University Press, 1997), 252.

affinities.[14] To become more adaptive, the armed forces would have to develop unfamiliar and uncomfortable cooperative characteristics founded on trust, the open flow of information, and a willingness to embrace technological innovation. Time-honored hierarchies would have to be deliberately blurred so that creativity could percolate from the ground up. Dogmatic doctrine could no longer hold leaders hostage to a prescribed set of actions. Still, Vietnam lingered as a painful example of the deliberate and wholesale "unlearning" of valuable skills, lessons, and traditions. There could be no blank page or clean slate; the defense community would have to respect the lessons of history as they purposefully reconfigured their still-valuable organizational components to support complex operations in a multifaceted environment.

The military knew that it would need to maximize the combined potential of the service components and began in 1999 by establishing the United States Joint Forces Command (USJFCOM) as the agency to implement this crucial change. One of USJFCOM's first challenges was to develop a means to rapidly deploy a situation-tailored joint command cell with associated joint forces that would be prepared for and effective at immediate crisis response. The prototype organizations that emerged were a Standing Joint Force Headquarters (SJFHQ) for crisis planning and readiness and the Joint Task Force (JTF), comprising a headquarters (HQ) with assigned service and functional components.

The SJFHQ operates under a high-ranking director and supporting Command Group staffed by joint-qualified military and civilian personnel. The organization comprises cross-functional teams—operations, plans, information superiority, and knowledge management—that accomplish daily mission requirements. These teams operate within a knowledge-based environment that emphasizes seamless, cross-functional collaboration between the teams, with the regional combatant command staffs and components, and with other external agencies.[15] In pre-crisis, the SJFHQ serves as a planning staff element that identifies likely future crisis scenarios, then establishes

---

[14] Michael Fitzsimmons, "Whither Capabilities-Based Planning," *Joint Forces Quarterly,* 2007;44:101–105.

[15] Major General Gordon C. Nash, U.S. Marine Corps, "Doctrinal Implications of the Standing Joint Force Headquarters (SJFHQ)," The Joint Warfighting Center Joint Doctrine Series, Pamphlet 3, June 16, 2003, 7–8.

and maintains situational understanding and planning options for critical geographic areas designated by a combatant commander.

When an actual crisis emerges, the operational commander must determine whether to build and deploy a JTF. Unlike the SJFHQ, JTFs and their headquarters are ad hoc organizations established on a geographic area or functional basis when the mission has a specific limited objective.[16] For events that are limited in duration and scope, the commander may opt to designate the SJFHQ as the core of the JTF HQ. More commonly, however, essential portions of the SJFHQ accelerate the transition of a service operational HQ to a JTF HQ, which is equipped with so-called plug-and-play force packages that are ready to go and particularly well-suited to the crisis at hand. From 2005 to 2008, USJFCOM SJFHQ core elements Alpha and Bravo deployed domestically to JTF Katrina and supported Multinational Forces Iraq, Combined Disaster Assistance Center Pakistan, JTF Lebanon, International Security Assistance Force Afghanistan, and the Combined JTF Horn of Africa.[17]

One of the greatest challenges for every JTF HQ is how to quickly grasp the situation in the midst of a crisis response. The staff needs time to achieve full situational understanding and become functionally effective amid a maelstrom of hasty deployment, unfamiliar players, imminent resource demands, and sometimes conflicting or confused directives from outside the immediate operational space. Operational experience and demand over time demonstrated that a more agile, responsive, and tailorable organization than the SJFHQ was required. On October 1, 2008, the SJFHQ adapted and transitioned to a new Joint Enabling Capabilities Command (JECC).[18]

Similar to its predecessor, the "JECC serves as the USJFCOM subordinate command responsible for providing forces to newly-established joint force headquarters that can rapidly enable critical

---

[16] Joint Publication 3-33: "Joint Task Force Headquarters" (February 15, 2007). Available at I-3. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_33.pdf

[17] "Standing Joint Force Headquarters Core Element (SJFHQ-CE)." U.S. Joint Forces Command. Fact Sheet. (Norfolk, VA: 2005).

[18] Courtney E. Howard, "USJFCOM Transitions Standing Joint Force Headquarters," USNORTHCOM Bulletin Board, September 30, 2008. Available at http://community.mae.pennnet.com/group/bulletinboard/forum/topics/2108638:Topic:1845.

command and control capabilities."[19] The joint-enabling capabilities available to combatant commanders include Joint Deployable Teams with capabilities in four critical areas: operations, plans, information superiority/knowledge management, and logistics. In addition to these core staff teams, the JECC offers enabling capabilities in a Joint Communications Support Element, Joint Public Affairs Support Element, and Intelligence–Quick Reaction teams.[20] The seven types of deployable teams can immediately offer joint structure, immediate availability, and mission-specific planning and intelligence capabilities, which provide the JTF HQ with the means to rapidly determine its courses of action and prepare and deploy an effective response.[21]

The SJFHQ and JECC organizational innovations have improved joint response at the regional and operational level, but their role is really to identify, recommend, and augment the requirements needed by a service-dependent JTF HQ for effective crisis response. Joint combatant commanders, with the exception of Special Operations Command, possess very few organic resources and rely almost entirely on personnel and assets from their constituent services to manage their areas of responsibility. Although all of the services are starting to embrace jointness in practice, contemporary pundits question the dependence on individual services to provide the capabilities the JTF HQs need, decrying it as wasteful, competitive, and redundant. Many critics suggest a more centrally controlled process to develop and manage joint capabilities—one that emphasizes efficiency and interdependence over the current characteristics of service specialization, limited organic sustainability, and interoperability.[22]

This option, though inarguably more cost-effective and joint-spirited, is not without its own risks. If the current, service-oriented capability packages are to be homogenized through joint capability development, over time the unique domain affinities (sea, air, land), institutional experiences, cultures, and lessons learned will become diluted. Service distinction and competition, as well as cooperation, can

---

[19] Joint Forces Command, "Joint Enabling Capabilities Command." Available at http://www.jfcom.mil/about/com_jecc.html.

[20] Ibid.

[21] Douglas K. Zimmerman, "Understanding the Standing Joint Force Headquarters," *Military Review* 2004;(July-August):28–29.

[22] Kathleen H. Hicks et al., *Transitioning Defense Organizational Initiatives: An Assessment of Key 2001-2008 Defense Reforms* (Washington, DC: Center for Strategic and International Studies, 2008), 56–64.

spur innovation and produce novel concepts when well-managed. Moreover, enforcing joint interdependence over joint interoperability risks single-point failures that jeopardize mission success. The long-term solution may be to promote joint development for universally applicable capabilities while retaining those distinct service-specific assets that preserve effective institutional roles for the U.S. Army, Navy, Air Force, and Marines.

The JECC and its predecessor provide a cogent example of how leadership, composition, structure, and responsibilities can be carefully shaped to better respond to the conditions imposed by the operational environment. In the commercial sector, Google offers a more profound example of shaping, in which the organization not only adapts to respond to crises in a rapidly changing competitive environment but also strives to incorporate the environmental conditions and its resident enterprises into its own organizational architecture. Google's mission "to organize the world's information and make it universally accessible and useful"[23] is a bold statement of transcendence of the competitive state to a space where goals and accomplishment are measured in absolute terms and the innovations of peers are viewed as collective opportunity. Shared information, and particularly networked information, is at the same time Google's product, mantra, and operational domain.

Google's organizational structure is an amazingly simple hub-and-spoke construct, with Google as the self-described information "keystone" that connects information suppliers (media, academia, industry, and individuals) with consumers, advertisers, and innovators to populate an "innovation ecosystem." When a non-Google innovator creates a new information product or platform, rather than attempting to thwart the "competitor," Google attempts to incorporate the new contributor into the network. Given the incentives—access to Google's information tools, marketing data, and revenue-sharing, among others—few would-be competitors can resist Google's magnetism. In fact, in Google's flourishing innovation ecosystem, competition has become passé, replaced by a "mash-up" of diverse information products and services that pass fluidly through traditional organizational boundaries to the mutual benefit of all stakeholders.[24]

---

[23] http://www.google.com/enterprise/whygoogle.html
[24] Bala Iyer and Thomas H. Davenport, "Reverse Engineering Google's Innovation Machine," *Harvard Business Review* 2008;86(4):59–68.

Google is now hosting the Android software platform as one emerging means to offer a diverse array of information-based capabilities in one convenient consumer tool. Android is an open-standards telecommunication platform that not only offers free Google products but also combines the capabilities of a range of available tools to create a consumer-responsive experience. For example, Android can combine the information in the user network's "contact" database, GPS applications, and Google Maps to allow Android users to locate friends in the Android network or automatically send alerts when an Android contact is within a designated geographical range. Without much imagination, the potential uses for this application could extend well beyond social networking to provide parents the ability to monitor children, allow victims of violent crime to avoid paroled offenders, or assist first responders in arriving quickly to a medical emergency. Though some of these technologies are available today, they are prohibitively expensive for broad public use. Android offers these and many other capabilities as a free feature, while simultaneously using its "open standards" status to encourage future Android-supported innovation.[25]

Act: Exploiting the Time-Information Advantage

The habit of control must yield to the power of networking.[26]

In today's information-rich environment, organizational shaping must work with informed reasoning to facilitate effective planning and action. Global information networks provide unprecedented opportunities to meld intuition and reasoning for rapid and adaptive decision-making. To benefit fully from this opportunity, however, organizations must be collaborative, decentralized, and pliable. In a diffuse and fluid competitive environment, centralized decision-making may be fatally unresponsive; in contrast, a "need-to-share" organizational mindset, supported by a distributed information network, can give leaders and managers in the field unobstructed access to information, the authority to act, and opportunities for collaboration, helping them gain a time-information advantage over their opponents.

There are four essential cognitive capabilities that must be functioning harmoniously to realize the time-information advantage:

---

[25] http://www.android.com
[26] Gompert, "Heads We Win," xi–xii.

anticipation, opportunism, decision speed, and learning in action.[27] Intuition provides initial direction, creating the opportunity to gather information and reason rapidly via networks to anticipate future conditions. Accurate anticipation sustains ownership of the initiative so that fleeting opportunities can be exploited through rapid-adaptive decisions. Through information-enabled anticipation, opportunism, and rapid-adaptive decision-making, organizations can gain a potentially decisive time-information advantage over competitors. Time saved through anticipation is used to gain information; then superior information is exploited to gain more time. Meanwhile, learning and adapting "on the fly" ensures that organizations do not fall into complacency or predictable actions.

The Federal Aviation Administration's collaborative decision-making project shows how decisions reached through well-informed teamwork can lead to effective action. Begun in 1990, the collaborative decision-making initiative is an effort to improve air traffic management through information sharing between industry stakeholders in "government, general aviation, airlines, private industry and academia who are working together to create technological and procedural solutions to traffic flow problems that face the National Airspace System (NAS)."[28]

Collaborative decision-making participants cooperate and share information to increase their situational awareness, and thus their capacity for collective decision-making. Through an actively maintained and user-updated Intranet, all of an airport's partners share the same operational picture, which in turn dramatically improves the timely anticipation and mitigation of potential scheduling conflicts, smoothes passenger flow between terminals, and alerts the entire aviation network to potential hazards. This network also serves as an invaluable data repository and analysis tool that automatically collects and processes information to streamline airspace flow and flight scheduling. Automated information management has compressed 90 days' worth of data analysis into as little 30 minutes.[29] By sharing what

---

[27] Ibid, xi.

[28] Federal Aviation Administration, "Collaborative Decision-Making Leadership Guide" (January 6, 2009). Available at http://cdm.fly.faa.gov/whatscdm/cdmdocs.html [Accessed March 10, 2009].

[29] Terence R. Thompson et al., "Terminal-Area Throughput: Measuring Capacity and Robustness," Eurocontrol ATM R&D Symposium white paper, Budapest, June 2003.

had long been considered proprietary industry data via an inclusive information network, the entire aviation community has benefited from enhanced awareness, efficiency, and cost savings, and passengers have been spared an estimated 50,000 hours of air delays since the program's inception.[30]

A similar catharsis has occurred in the defense sector. The current conflict in Afghanistan demonstrates how a technologically enabled time-information advantage has helped shape rigid military organizational structures to be more agile and responsive at the operational level. Following successful major combat operations in 2002, U.S. operational tasks shifted to nation-building—an unfamiliar and daunting task. Because the security environment was still deadly and domestic capacity nonexistent, it fell largely on an ill-suited military occupation force to rebuild an Afghan central government that could establish and maintain rule of law and good governance. The capability requirements for this extremely complex task were extensive, dynamic, and unfamiliar to military planners and leaders. Numerous environmental uncertainties, and especially the influence of key figures such as President Hamid Karzai and Taliban leader Mullah Omar, loomed large and even appeared to hold success or failure in the balance.[31]

The complexities associated with propping up a viable central government in Afghanistan while maintaining interim stability through a rotating assortment of multinational and interagency players has since been addressed in large part by the U.S. creation of a new operational-level organization: the provincial reconstruction team (PRT).[32] A radical departure for the military, a PRT is designed as a more or less "flat" organization, wherein military representatives comingle with peer-level civilian officials from the U.S. departments of State, Agriculture, and Treasury as they cooperate closely with Afghan agencies and nongovernmental and international aid organizations. The exact organizational compositions, hierarchies, coverage areas, and tasks vary widely among a few dozen of these malleable "people-

---

[30] Ibid.

[31] Kathleen Hicks and Eric Ridge, "Planning for Stability Operations: The Use of Capabilities-Based Approaches," a report of the International Security Program (Washington, DC: Center for Strategic and International Studies, 2007), 16–22.

[32] James Dobbins et al., *America's Role in Nation-Building: From Germany to Iraq* (Santa Monica, CA: RAND, 2003), 136.

centric" networks, according to each military commander's comprehensive needs assessment, the PRT's primary regional challenges, and even the personal relationships and interactions of its stakeholders.

Multinational partners in the North Atlantic Treaty Organization's International Security Assistance Force have since adopted their own renditions of the PRT model and further emphasized the diverse organizational possibilities inherent to the construct. As the Netherlands Defence Staff eloquently observed, "Working in PRTs is a complex and demanding task, which makes detailed understanding of the mission, the environmental conditions and the formal and informal influential actors essential. PRTs are not based on a rigid doctrinal concept and the concepts behind reconstruction and the military contribution to it are in a state of rapid development. Concepts related to PRTs are therefore also evolving constantly."[33] Despite or perhaps because of these ever-shifting requirements, the PRT model continues to endure and evolve in one of the globe's most intractable disruption zones, ever striving to improve agility and unified responsiveness in the face of uncertainty, austerity, and hostility.

Evaluate: Defining, Determining, and Enhancing Success

> The understanding of instability is . . . derived from analysis fed from many sources . . . information that feeds these plans is vulnerable to subjectivity, is rarely quantifiable, is difficult to measure and is infrequently reviewed.[34]

PRTs offer invaluable insights into the importance of a regular evaluation of environmental conditions, shaping efforts, and action outcomes. The joint force commander must expect that, however carefully conceived, his initial operational design might prove inadequate. The PRT plan must incorporate means of continuously assessing the results of operations in relation to expectations and be

---

[33] Joint Doctrine Bulletin 2008/01, "Provincial Reconstruction Teams' deployment in Afghanistan," Netherlands Defence Staff, Defence Staff/DOBBP/Doctrine Division, The Hague (2008): iii. Available at http://www.yourdefence.nl/file.php/1/moddata/forum/2/247/JDB_0801_PRT_OPS_English_version.pdf.

[34] T. R. Brewer, "Tactical Conflict Assessment Framework: Trial Report" (TF Helmand, NATO International Security Assistance Force, 2008), iii.

prepared to modify operations when the two diverge. By probing the situation, operations themselves become a way of testing early assumptions and expectations.[35]

In Afghanistan, the United Kingdom is part of the International Security and Assistance Force, with a charter to stabilize Afghanistan and "set it on a path toward economic development and increased political freedoms."[36] Britain's Afghanistan PRT, located in Helmand province, comprises representatives and resource contributions from its Ministry of Defence, Foreign and Commonwealth Office, and Department for International Development. The British PRT's activities in Helmand are driven by the Helmand Road Map, a 2-year plan under annual evaluation. According to the plan, civil and military activities center on five main geographical areas, controlled by a politically led counterinsurgency campaign. This approach depends on the consent of the population and its support for the government at least as much as on holding ground or eliminating the Taliban. For this reason, military tasks are designed with a "civilian effects" purpose.[37]

The complexity of Afghan social networks adds an additional wrinkle to the achievement of a time-information advantage. The civil environment is characterized by an innate mistrust of government, strong tribal loyalties and bitter clan rivalries, and a commercial exchange system that is so foreign as to be anathema to Westerners. Western, and particularly military, organizations are notoriously action-oriented, and leaders feel compelled to move quickly—even prematurely—based on initial impressions of need. In Helmand, leaders soon learned that this well-intentioned desire for rapid assistance had to be tempered with exhaustive, highly formalized discussions with trusted local Afghani leaders. For instance, the perceived need to restore reliable irrigation to the agriculture-dependent province had to take into consideration the near-exclusive cultivation of opium poppies as the primary cash crop. If restoration of the irrigation system were not

---

[35] Admiral M. G. Mullen, "Capstone Concept for Joint Operations," version 3.0 (Washington, DC: Joint Chiefs of Staff, 2009), 14. Available at http://www.dtic.mil/futurejointwarfare.

[36] Robert Perito et al., *Provincial Reconstruction Teams: Lessons and Recommendations* (Princeton, NJ: Woodrow Wilson School of Public and International Affairs, Princeton University, 2008), 42–46.

[37] Peter Dahl Thruelson, "Counterinsurgency and a Comprehensive Approach: Helmand Province, Afghanistan," *Small Wars Journal,* 2008;7. Available at http://smallwarsjournal.com/mag/docs-temp/100-thruelsen.pdf.

accompanied by incentives for legitimate farming and poppy eradication, assistance efforts would inadvertently fuel opium production. Similarly, the intuitive move to establish a powerful military presence proved counterproductive because it fueled antioccupation sympathies and Taliban recruitment. Clearly, the challenge was not simply to take action quickly but to exploit information to take the correct actions.[38]

To synchronize actions to be both rapid and effective, the Road Map demands close cooperation between civil and military stakeholders and frequent interaction with local Afghan leaders. The Road Map further describes eight steps of integrated action.

Step 1: Begin a civilian-led effort to prioritize the various actors' goals.

Step 2: Identify those collective actions necessary to achieve desired effects.

Step 3: Synchronize roles and responsibilities for all participants.

Step 4: Analyze and approve available resources.

Step 5: Develop an integrated resource plan.

Step 6: Carry out preparations and tactical planning.

Step 7: Execute integrated civil–military operations.

Step 8: Consolidate and evaluate desired effects.[39]

Priorities will often originate from discussions with trusted Afghan tribal leaders. Close daily interaction between the top civilian and military leaders ensures they share a common understanding of the immediate situation and assists the civilian PRT chief in assigning weights and directing focus. This cooperative feedback and immediate-decision capability may lead to rapid adjustments in the delivery of civilian services and security without necessitating a formal planning

---

[38] Rene L. Cote, "Data-Driven Stabilization: The Process of Selecting Reconstruction and Development Efforts," 4th Civil Affairs Group, U.S. Marine Corps, Anacostia Annex, Washington, DC, July 13, 2007, 2–3. Available at http://www.civilaffairsassoc.org/Data-Driven%20Stabilization.pdf [Accessed March 5, 2009].

[39] Thruelson, "Counterinsurgency," 8.

process. Similarly, in hostile environments where security is the overriding priority, civilian actors may have little or no involvement in the planning and delivery of security services, which lie almost exclusively under military purview.

In tandem with this internal synchronization, TF Helmand adopted a structured approach to collecting information that could first identify the root causes of instability or conflict, then determine whether the actions taken by the PRT were achieving their intended effects. The PRT opted to adopt an assessment tool developed by the U.S. Agency for International Development: the Tactical Conflict Assessment Framework (TCAF). The agency describes the TCAF as "a standardized diagnostic tool designed for use by both military and civilian personnel. It is employed to gather information from local inhabitants to identify the causes of instability or conflict in tactical areas of operation. This information helps identify, prioritize, monitor, evaluate, and adjust civil–military programming targeted at diminishing the causes of instability or conflict."[40] British leaders on the ground in Helmand confirm that this description fits their experience. According to Lieutenant Colonel Richard Wardlaw, commander of the Task Force's 52 Brigade Engineers, "TCAF does more than just enable us to establish what the main problems are that cause instability. If you then keep asking those questions, over time you also get measurement of effect."[41]

The task force began with a core assessment. Using military foot patrols that had already established trust with the local population, the TCAF assessment gathered essential information using four basic questions:

1. Have there been any changes in the village population in the last year? Why?
2. What is the most important problem facing the village?
3. Who do you believe can solve your problems?

---

[40] "Tactical Conflict Assessment Framework," USAID Military Affairs Web site. Available at http://www.usaid.gov/our_work/global_partnerships/ma/tcaf.html.

[41] As quoted by James Holland in "I Have Seen the Way Open for Hope in Helmand," *Telegraph*, December 15, 2008. Available at http://www.telegraph.co.uk/comment/3554496/I-have-seen-the-way-open-for-hope-in-Helmand.html.

4. What should be done first to help the village?[42]

The open-ended nature of the questions encouraged dialogue and opportunities for locals to air grievances and concerns and, perhaps most important, capture their notions for a brighter future. These carefully framed questions also provided important insights about perceptions of the PRT's mission and presence, and where local trust and loyalty resided. The same questions were repeated regularly over an extended period, so that effects from initial actions could be validated, fine-tuned, supplemented, or replaced by subsequent actions. Over time, the survey results identified and confirmed root causes and greatly facilitated the tracking of quantifiable trends and outcomes.

TCAF is already producing results in Helmand. Results from data gathered in both Lashkar Gah, the provincial capital, and the city of Sangin using the TCAF evaluation tool indicated that earlier assumptions about each city's grievances and needs had been quite wrong. Moreover, results in the two places were very different, showing how wide local differences can be. Based on this evaluation and new understanding, the Helmand PRT is reshaping reconstruction and development initiatives in these two cities so that actions will be more effective. Like all complex adaptive organizations, the Helmand PRT will continue to evolve. Based on the lessons learned in Helmand, military–political analysts are already suggesting two new organizational innovations for future PRT deployments: "mobile PRTs" that could follow troops immediately after combat operations, and "indigenous PRTs" led and populated by local civilians and augmented with foreign capacity-building and support.[43]

The U.N.'s World Bank is also exploring more meaningful metrics that might reveal more effective approaches for combating poverty. World Bank concept leaders have made a remarkable departure from traditional poverty assessment. World Bank is now experimenting with a capabilities-based assessment model that is based on a comprehensive quality-of-life evaluation in place of a purely income-based "poverty-line" metric. The central contention is that poverty is defined more succinctly as a "deprivation of basic capabilities rather than merely a lowness of incomes."[44]

---

[42] Cote, "Data-Driven Stabilization," 3.

[43] Perito, "Provincial Reconstruction Teams," 46.

[44] Sanjay Reddy et al., "Inter-Country Comparisons of Poverty Based on a Capability Approach: An Empirical Exercise," Q-Squared working paper 28.

The traditional infusions of money into the national coffers of poverty-stricken nations based on purely monetary metrics have too often yielded unexpected and even counterproductive results: inflation, corruption, and cultures of dependency. Recognizing this, in 2006, the World Bank initiated a limited-scope experiment to determine whether capabilities-based metrics might produce better solutions. Acknowledging that a number of factors contributed to the condition of poverty (e.g., availability of food, shelter, and security), the experiment focused on one indisputable capability requirement, "the capability to be adequately nourished" to establish one potential new poverty metric for comparison with the traditional income-based poverty line, using statistical data from Nicaragua, Tanzania, and Vietnam. The measure, caloric intake, was assumed to have a fixed criterion for adequate nourishment, set at 2,100 kilocalories, which established a sort of "food poverty line." The experiment measured caloric intake in each of the three countries, taking into account, to the extent possible, the comparative nutritional values of each country's typical diet.

The results of the experiment revealed a notable divergence in these countries' global poverty rankings with the application of the "food poverty" measures when contrasted against the "income poverty" line. In Vietnam, "nutritional" poverty was 84% higher than its comparable monetary indicator, whereas Tanzania enjoyed a 45% decrease in poverty with the application of the "food poverty" line.[45]

This experiment is important primarily in that it illustrates the need to determine root causal relationships for effective evaluation. The World Bank experimentation team acknowledged that adequate sustenance was only one of many true poverty indicators, but that, in general, "the possession of elementary capabilities provides an approach to international poverty comparison and aggregation that is both coherent and meaningful, unlike existing money-metric approaches." The radical, but retrospectively obvious, conclusion that access to money is only one contributor to a holistic set of basic "capabilities gaps" that define poverty should lead to more effective World Bank approaches. The results from this experiment and future capabilities-based evaluations will contribute to a more comprehensive

Toronto: Center for International Studies, 2006, 1. Available at http://www.sarpn.org.za/documents/d0002281/index.php.

[45] Ibid., 3-4, 16–18.

understanding of poverty, which should lead to more effective shaping of conditions to enhance poverty eradication actions.

Conclusion

Information Age organizations are complex and dynamic "living" entities that interact with and influence their environments. People are the building blocks: creative and intelligent components with a latent ability to produce not only stipulated outcomes but also novel ideas and achievements. When visualized and treated as complex adaptive systems, organizations more readily take advantage of emergent technologies, as well as the human potential to innovate and adapt. To realize their full potential, complex adaptive organizations must also be capable of managing and even encouraging change.

Adaptive organizations possess markedly cooperative characteristics that operate on trust, the open flow of information, and a readiness to incorporate technological innovation. They are not based on or hostage to a set of inviolate roles, policies, and structures that form the rigid pillars for success. Rather, they purposefully reconfigure these important organizational components to support new projects or activities. Deliberate adaptation demands an improved ability to understand the operating environment and underlying causal relationships, to shape the organization and its contextual conditions for optimal performance, to act effectively to exploit opportunities to exert influence, and to evaluate outcomes to sustain competitive advantage. Actions are followed by a careful assessment of results in relation to expectations, which enhances understanding and leads to subsequent adaptations.

In the Information Age, intuition must be integrated with reasoning for optimal decision-making ability. Intuition alone may not be reliable in unfamiliar situations, whereas reasoning can be aided tremendously by networked information. Four cognitive abilities are particularly important in organizational adaptation: understand → shape → act → evaluate. These cognitive abilities must not be concentrated among the few at the organizational core but, instead, distributed across the many in the field, who must in turn be trusted with unfettered access to the information network, authority to act, and opportunities to collaborate horizontally without deference to a higher authority. In complex adaptive organizations, the comfort of control must yield to the power of innovation.

About the Contributors

Torsten Björkman is a senior management consultant and evaluator and professor emeritus of leadership at the Swedish National Defence College. At the college, Björkman has had numerous assignments, including head of the Department of Leadership. He also is professor emeritus in work sciences from the Swedish Royal Institute of Technology and has an educational background from the University of Uppsala with a Ph.D. in sociology. His most recent assignment is an ongoing comparative organizational analysis of the military headquarters of the Nordic countries—Norway, Denmark, Sweden, and Finland.

Louise Carver, BA (HONS), is an independent management consultant specializing in training development, design, and delivery; culture change; and stakeholder engagement. After completing a degree in German and Scandinavian Studies, Louise joined the Royal Air Force as a training and development officer and worked in various areas including operations, housing, and personnel management. She retired in 2007 to set up her own consultancy business. She is a chartered member of the Chartered Institute of Personnel and Development and an accredited Belbin Team Roles facilitator.

Jeffrey L. Caton (Col, USAF) is the defense transformation chair and a professor at the U.S. Army War College, Carlisle, Pennsylvania. He supports course development and seminar teaching to prepare selected leaders for strategic security roles. He has commanded at the squadron and group level in the U.S. Air Force. His duties over 27 years include space and missile operations, joint specialty operations and planning, and acquisition engineering, test, and program management.

Walter L. Christman is associate professor of global public policy at the Naval Postgraduate School and a visiting fellow of the Center for Technology and National Security Policy at the U.S. National Defense University. Previously, he served for over 20 years as a career civil servant of the U.S. Department of Defense and, during that period, for 10 years in Geneva, Switzerland, in a diplomatic capacity. He is a pioneer in the development of collaborative networks for international security cooperation.

Ralph Doughty is professor and chair of interagency and multinational studies at the U.S. Army Command and General Staff

College at Fort Leavenworth, Kansas. He holds a Ph.D. in mechanical engineering from the University of Alabama and is a retired U.S. Army major general who has commanded at battalion, brigade, and division level. He was president of a civilian consulting company in the United States for 10 years before returning to Fort Leavenworth.

Henrik Friman is professor and research director at Swedish National Research Agency. He has a scientific background, with a Ph.D. in strategic management from Stockholm University, School of Business. Dr. Friman is an army reserve officer with multiple command assignments. He is a fellow of the Swedish Royal War Academy and holds a professorship at the U.S. Naval Postgraduate School Center of Innovation and Experimentation.

John Garstka is a Senior Analyst in the Directorate of Communications and Networking Programs and Policy, ASD(Networks and Information Integration), U.S. Department of Defense. Prior to joining ASD(NII) he worked in OUSD(Policy), the Office of Force Transformation, and the Directorate for C4 Systems on the Joint Staff. He has a background in systems engineering and analysis with a M.S. in Engineering-Economic Systems from Stanford University. He is a Distinguished Graduate of the U.S. Air Force Academy and served on active duty in the U.S. Air Force for 10 years and in the US Air Force Reserve for 15 years. He has written and spoken extensively on the topics of transformation and network-centric operations.

John P. Geis II (Col, USAF) is the director of the Air Force Center for Strategy and Technology and is an associate professor of international security studies at the Air War College. Colonel Geis' career spans the fields of fighter, training, education, and special operations. Colonel Geis has an undergraduate degree in meteorology, three Master's degrees in the social sciences, and a Ph.D. in political science from the University of Wisconsin.

Ted Hailes (Col [R] USAF) retired from the U.S. Air Force in 1996 and is currently the transformation chair at the Air University, an Air War College faculty member, and cofounder of the Center for Strategy and Technology. His research is focusing on accelerating technological change. On active duty, he flew fighter aircraft and had multiple command and staff positions. Civilian education includes a B.A. in European history and a M.S. in international relations.

Grant Hammond is the dean of the NATO Defense College in Rome, Italy. With a B.A. degree from Harvard, and a M.A. and a Ph.D.

from Johns Hopkins University, he has spent 20 years in professional military education (U.S. Air War College, Center for Strategy and Technology). The author of numerous articles, book chapters, and U.S. Government studies, he has published three books and specializes in the field of strategy, international security, future conflict, and adaptive learning.

Richard Hughes is the transformation chair at the U.S. Air Force Academy. He was head of the academy's Department of Behavioral Sciences and Leadership for 10 years, and before becoming the transformation chair in 2007, he served for 12 years with the Center for Creative Leadership. His research interests include strategic leadership and organizational culture change, and he is senior author of a widely used university textbook on leadership, and coauthor of a book on strategic leadership. He has a Ph.D. in clinical psychology from the University of Wyoming.

Scott Jasper teaches courses in international defense transformation in the Center for Civil-Military Relations at the Naval Postgraduate School. As a U.S. Navy captain, he served as the deputy for joint experimentation at Headquarters, U.S. Pacific Command. A U.S. Naval Academy graduate, he holds an M.B.A. from San Jose State University and a M.A. from the Naval War College. His first volume is *Transforming Defense Capabilities: New Approaches for International Security* (Lynne Rienner, 2009).

Sandra M. Martínez works in leadership development and organizational transformation. She earned a Master's degree with distinction in Latin American studies and international business from the University of New Mexico and a doctorate in business administration from New Mexico State University. She was a research associate for the GLOBE project of the Wharton School; later, she served as chair of defense transformation at the U.S. Army War College, where she initiated research on emergent leadership. At this time, she resides in Honduras and holds appointments at both Zamorano University and the Cebrowski Institute of the Naval Postgraduate School.

Scott Moreland is a lecturer and research associate at the Center for Civil-Military Relations at the Naval Postgraduate School. He is a retired U.S. Army officer and earned his Master's degree in international peace and conflict resolution from American Military University.

Derrick Neal is professor of defence strategic change with Cranfield University at the Defence Academy of the United Kingdom. He has an engineering background with a Ph.D. in fluid mechanics and an M.B.A. from Cranfield University. Professor Neal has 20 years of industrial experience in a variety of roles and has been at Cranfield University since 1998. He teaches, researches, and publishes in the areas of strategic/change management within a defense context.

Terry J. Pudas is a senior research fellow at the U.S. National Defense University Center for Technology and National Security Policy, where his work is focused on transformation and related national security issues. In September 2001 he was appointed the deputy director of the newly created Secretary of Defense Force Transformation Office. He retired from the U.S. Navy in September 2001 with over 32 years of service after serving as the deputy and executive assistant to the president of the Naval War College in Newport, Rhode Island. He was designated a naval aviator in May 1971 and served in numerous fighter squadrons.

Andrew Stricker serves as the distributed learning architect for Air University by helping to design, develop, and implement advanced and emerging learning technologies and standards into U.S. Air Force educational and professional military education programs. Previously, Andrew served Vanderbilt University as associate provost for innovation through technology. He was responsible for working with academic, technology, and administrative leaders to prioritize, plan, and execute the infusion of technologies and enabling innovations for transforming learning, teaching, and research. His graduate work was conducted at Texas A&M University and Yale University.

Jon Stull is an associate professor of transformation and interagency initiatives with the Joint Forces Staff College of the National Defense University located in Norfolk, Virginia. He is a graduate of Colgate University and holds advanced degrees from Salve Regina College and the U.S. Naval War College. Professor Stull, a retired colonel who spent 30 years in the U.S. Marine Corps, teaches joint, interagency, and multinational planning to midgrade military and civilian officers.

Linton Wells II serves as Transformation Chair and distinguished research professor at the U.S. National Defense University. Previously he served 16 years in the Office of the Secretary of Defense, including 2 years as the Defense Department chief information officer. Dr. Wells served 26 years in the U.S. Navy, commanding twice at sea. He

coordinates the STAR-TIDES international knowledge-sharing research project on sustainable support to stressed populations (http://www.star-tides.net).